# REPORT DOCUMENTATION PAGE

AFRL-SR-BL-TR-99-

0083



| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | 17 Feb 99 | Final Report 1 Aug 98 - 31 Jan 99 |

**4. TITLE AND SUBTITLE**
Novel Mathematical/Computation Approaches to Image Exploitation

**5. FUNDING NUMBERS**
F49620-98-C-0043

**6. AUTHOR(S)**
Dr. Richard Tolimieri, Dr. Myoung An
Dr. Ta-Ming Fang, Professor Bryant York

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Massachusetts Technological laboratory, Inc.
330 Pleasant Street
Belmont, MA 02478

**8. PERFORMING ORGANIZATION REPORT NUMBER**
MTL 0004Z

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Air Force Office of scientific Research
801 North Randolph St., Room 732
Arlington, VA 22203-1977

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Distribution unlimited

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** *(Maximum 200 words)*

A study of the harmonic analysis of finite abelian groups and a class of finite nonabelian groups is presented.

The restriction to groups of the form $G = A \leftthreetimes B$ and their generalizations permit harmonic analysis to proceed by abelian group character theory. This results in: 1) a direct link with abelian group harmonic analysis and consequently with physical interpretation. 2) automatic procedures for constructing direct sum decompositions of the group algebras into irreducible invariant subspaces. 3) algorithms for computing bases of irreducible, invariant subspaces and spectral bases compatible with direct sum decompositions. 4) fast algorithms for representing data over spectral basis. 5) an extensive new class of fast unitary transforms for data analysis.

Extensive numerical experiments have shown the potential power of this technique for texture analysis and feature extraction in the presence of noise.

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| harmonic analysis, abelian groups | 80 |
| | 16. PRICE CODE |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| U | U | U | UL |

# Novel Mathematical/Computational Approaches to Image Exploitation

Research and Development

**Final Technical Report**

Reporting Period: 01 August, 1998 - 31 January, 1999

Contract # F49620-98-C-0043

Sponsored by

Air Force Office of Scientific Research (DOD)
Defense Small Business Technology Transfer Program

Principal Investigator: Dr. Richard Tolimieri

Contractor: Massachusetts Technological Laboratory, Inc.

Business Address: 330 Pleasant Street, Belmont, MA 02478

Research Institution: College of Computer Science, Northeastern University

Business Address: 161 Cullinane Hall, Boston, MA 02115

Effective Date of Contract: 1 August, 1998
Contract Expiration Date: 15 March, 1999



**Submitted by**

Dr. Ta-Ming Fang
Massachusetts Technological Laboratory, Inc.
(617)484-2296; (617)484-7314 (Fax)

16 February, 1999

Disclaimer

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed, or implied, of the Air Force Office of Scientific Research or the U. S. Government.

# 1 Overview of Mathematical Accomplishments

We present a study of the harmonic analysis of finite abelian groups $A$ and finite groups $G$ of the form $A \leftthreetimes B$ , the semidirect product of a normal abelian group $A$ with an abelian group $B$. The theory easily generalizes to finite groups $A \leftthreetimes H$, where $A$ is a normal abelian group and $H$ is an arbitrary group whose harmonic analysis is known. In particular, it includes finite groups $A \leftthreetimes (B \leftthreetimes C)$, where $A$, $B$ and $C$ are abelian subgroups. This rich class of finite groups contains all crystallographic groups.

For the most part group algebras will be taken over the complex field (split case), but a section on group algebras of abelian groups over finite fields has been included as an indication of the methods that must be developed for applications to coding theory.

The restriction to groups $G = A \leftthreetimes B$ and their generalizations permit harmonic analysis to proceed by abelian group character theory. This results in

- a direct link with abelian group harmonic analysis and consequently with physical interpretation.
- automatic procedures for constructing $G$-invariant, irreducible $G$-invariant and direct sum decompositions of $\mathbf{C}G$, the group algebra of $G$ over $\mathbf{C}$, into irreducible $G$-invariant subspaces.
- algorithms for computing bases of irreducible $G$-invariant subspaces and bases compatible with direct sum decompositions of $\mathbf{C}G$ into $G$-invariant and irreducible $G$-invariant subspaces (spectral bases).
- $\overline{\text{fast}}$ algorithms for representing data, i.e., elements in $\mathbf{C}G$, over spectral basis.
- an extensive new class of fast unitary transforms for data analysis.

## 2 Introduction

From a mathematical perspective, a significant part of classical digital signal processing (DSP) can be viewed as topics in finite abelian group harmonic analysis [ 1, 6, 16, 4]. Fundamental DSP operations such as convolution and the Fourier transform can be identified with group algebra multiplication and group algebra direct sum decompositions into irreducible group invariant subspaces. This interplay, often implicit, has been responsible for fast algorithms such as the FFT [ 7], the use of FFT in computing large size convolutions and correlations, and more recently for the development of polynomial transforms [ 27, 25] for computing convolutions.

However pleasing, at least to the mathematically inclined, and useful this group theoretic approach to DSP, it is based on a seemingly magical relationship between DSP applications and finite abelian group harmonic analysis and the simplicity of this harmonic analysis. This magic can be explained by the powerful role played by abelian group characters in providing all that is required for finite abelian group harmonic analysis and the physical interpretation of these characters as frequency.

For some mathematicians, this group interpretation of DSP has raised the potential of an equally important application of nonabelian group harmonic analysis to DSP, especially in the construction of group transforms and group filers generalizing the classical Fourier transform and convolutional filters. The works of R. Holmes [ 14, 15], M. Karpovski and E. Trachtenberg [ 18] are the basis of much of the research in this direction. Similar ideas in coding theory have been introduced by F.J. MacWilliams [ 21]. These efforts have shown some promise but for the most part are more interesting to mathematicians than DSP engineers. A more successful application has been to fast algorithm design [ 22, 23, 2, 3, 10].

During the last ten years considerable effort has taken place to extend the success and range of applicability of nonabelian group methods to the design of new filters and spectral analysis methodologies [ 8, 9, 5], as an image processing tool [ 11, 13, 19, 20] and most recently as an image processing tool combined with graph theoretic modeling of image data [ 12, 24].

Many efforts at finding a significant role for nonabelian group theory in DSP and imaging applications as well as in coding and communication theory have been limited by some or all of the following.

- The choice of an appropriate group or groups in a given application is not obvious. Often the groups considered are those which are best known to the researcher.
- The lack of a large class of groups whose harmonic analysis is sufficiently understood for meaningful applications. Often the dihedral group with or without justification is the test example.

- The need to develop a conceptual framework which relates group harmonic analysis to physically interpretable results.
- Fast algorithms may exist but are difficult to code as they do not easily lend themselves to modification.
- Relevant models for applications which are not only a rephrasing of known methods or what is immediately available.

In the following three sections, we present a detailed account of finite abelian group harmonic analysis. This theory is well-known to most mathematicians but may not be familiar to DSP engineers. It is the starting point for the nonabelian group harmonic analysis developed in this work since as we will see both the abelian group and nonabelian group theories share many common features.

The finite nonabelian groups in this study have the form $G = A \leftthreetimes B$, the semidirect product of a normal abelian group $A$ with an abelian group $B$. Results easily extend to finite groups $A \leftthreetimes H$, where $H$ is an arbitrary group whose harmonic analysis is known. This includes finite groups of the form $A \leftthreetimes (B \leftthreetimes C)$, where $A$, $B$ and $C$ are abelian groups and in particular all crystallographic groups. In the applications part, we will see how these nonabelian groups provide for new classes of imaging and DSP models.

The language of group algebras usually over the complex field will be used throughout. Some readers may be more familiar with the identification of the group algebra $\mathbf{C}G$ with the space of all complex valued functions on $G$ under $G$-convolution. Harmonic analysis over $G$ usually includes a description of the (left) $G$-invariant and irreducible $G$-invariant subspaces and direct sum decompositions of $\mathbf{C}G$ into irreducible $G$-invariant subspaces.

For an abelian group $A$, complete answers to these problems can be given in terms of the characters of $A$. Moreover, these descriptions are especially simple. For example the irreducible $A$-invariant subspaces coincide with the one-dimensional subspaces spanned by the characters. The characters of $A$ determine an orthogonal basis of $\mathbf{C}A$ and the finite Fourier transform relates the delta basis $A$ of $\mathbf{C}A$ with the basis of characters of $A$. This is an extremely nice answer for applications since the characters of $A$ can be physically interpreted as frequencies.

For finite groups $A \leftthreetimes B$, the characters of $A$ and $B$ play an equally important but more complicated role in the harmonic analysis of $A \leftthreetimes B$. This theory is developed in section 6 and extensions to $A \leftthreetimes (B \leftthreetimes C)$ and beyond will be developed in time. We will have as a result *a large class of nonabelian groups with the potential of wide applicability to DSP and imaging whose harmonic analysis is known in detail. This harmonic analysis is based on abelian group characters which directly link this harmonic analysis to familiar DSP and imaging concepts.* Moreover we have developed

- algorithms for computing bases of irreducible $G$-invariant subspaces and

bases compatible with direct sum decompositions of $\mathbf{C}G$ into $G$-invariant and irreducible $G$-invariant subspaces (spectral bases).

- fast algorithms for representing data, i.e., elements in $\mathbf{C}G$ over spectral bases.
- an extensive new class of fast unitary transforms for data analysis.

The direct sum decompositions of $\mathbf{C}G$ studied in this work are closely related to but are significantly different from those leading up to the Fourier transform of $\mathbf{C}G$ [ 10, 26]. Our decompositions are finer but are not generally uniquely determined.

Throughout the mathematics part $A$ and $B$ denote finite abelian groups with composition given by multiplication. The identity is always denoted by 1 and the inverse of $x \in A$ by $x^{-1}$. The order of a set is the number of elements in the set.

For much of the general theory $K$ denotes a field, finite or infinite, whose characteristic does not divide the orders of $A$ and $B$. However for DSP and imaging applications, $K$ is the field of complex numbers. A section on group algebras of $A$ over finite fields is included as an indication of the methods used in applications to coding theory.


1. L. Auslander and R. Tolimieri, "Is computing with the finite Fourier transform pure or applied mathematics?," *Bull. Math. Soc.(N.S.)* **1**(6), 847-897, 1997.
2. U. Baum, "Existence and efficient construction of fast Fourier transforms for supersolvable groups," *Computational Complexity* **1**, 235-256, 1991.
3. U. Baum, M. Clausen and B. Tietz, "Improved upper complexity bounds for the discrete Fourier transform," *AAECC* **2**, 35-43, 1991.
4. R. Blahut, *Algebraic methods for signal processing and communications coding,* Springer-Verlag, NY 1992.
5. L. Beckett and P. Diaconis, "Spectral analysis for discrete longitudinal data," *Adv. Math.* **103** 1994, 107-128.
6. T.C. Carins, "On the Fourier transform on finite abelian groups'" *IEEE Trans., Comput.*, 569-671, May 1971.
7. J.W. Cooley and J.W. Tukey, "An algorithm for machine calculation of complex Fourier series," *Math. Comp.*, **19**, 297-301, 1965.
8. P. Diaconis, "A Generalization of spectral analysis of with applications to ranked data," *Ann. Stat.* **17**, 949-979, 1989.

9. P. Diaconis, *Group representations in probability and statistics*, IMS, Hayward, CA, 1988.

10. P. Diaconis and D. Rockmore, "Efficient computation of the Fourier transform on finite groups," *J. of AMS* **3**(2), 297-332, 1990.

11. D. Eberly and D. Wenzel, "Adaptation of group algebras to signal and image processing," *CVGIP: Graphical models and image processing* **53**(5), 1689-1711, 1996.

12. A. Figá-Talamanca and C. Nebbia, "Harmonic analysis and representation theory for groups acting on homogeneous tress," *LMS Lecture note series 162*, Cambridge U. Press, 1991.

13. Y. Fisher, E.W. Jacobs and R.D. Boss, "Fractal image compression using iterated transforms," *Image and text compression*, J. Storer, ed., 35-61, Kluwer Academic Press.

14. R. Holmes, "Signal processing on finite groups," *Technical Report 873*, MIT Lincoln Laboratory, 1990.

15. R. Holmes, "Mathematical foundations of signal processing II," *Technical Report 781*, MIT Lincoln Laboratory, 1987.

16. T.A.C.M. Kalker and L.A. Shah, "A group theoretic approach to multidimensional filter banks: theory and applications," *IEEE Trans. SP* **44**(6), 1392-1405, 1996.

17. M. Karpovski, "Fast Fourier transforms on finite nonabelian groups," *IEEE Trans. Comput.*, **C-26**(10), 1028-1030, 1977.

18. M. Karpovski and E. Trachtenberg, "Filtering in a communication channel by Fourier transforms over finite groups," *Spectral techniques and fault detection*, M. Karpovski, ed., Academic Press, NY 1985.

19. R. Lenz, "Using representations of the dihedral groups in the design of early vision filters," *Proc. ICASSP* **5**, 165-168, 1993.

20. R. Lenz, *Group theoretical methods in image processing* Springer-Verlag, NY 1987.

21. F.J. MacWilliams, "Codes and ideals in group algebras," *Combinatorial mathematics and its applications*, 317-328, R.C. Bose and T.A. Dowlin, eds., University of North Carolina Press, Chapel Hill, 1969.

22. D. Maslen and D. Rockmore, "Generalized FFTs'" *DIMACS Ser. in Disc. Math. and Theor. Comp. Sci.*, **28**, 183-237, L. Finkelstein and W. Kantor, eds., 1997.

23. D. Maslen and D. Rockmore, "Separation of variables and the efficient computation of Fourier transforms on finite groups, I," *J. of AMS* **10**(1), 169-214, 1997.

24. G. Mirchandani , R. Foote, D. Rockmore, D. Healy and T. Olson, "A wreath product group approach to image processing,", in preparation.

25. H.J. Nussbaumer, *Fast Fourier transform and convolution algorithms*, 2nd ed., Springer-Verlag, Berlin, 1982.

26. J.P. Serre, *Linear representation of finite groups*, Springer-Verlag, NY, 1977.

27. S. Winograd, "Arithmetic complexity of computations," *CBMS-NSF Regional Conf. Ser. Appl. Math., SIAM* **33**, 1980.

# 3 Characters of Finite Abelian Groups

A mapping $\tau : A \to K^\times$ is called a *character* of $A$ over $K$ if $\tau$ is a homomorphism of the group $A$ into the multiplicative group $K^\times$ of nonzero elements in $K$,

$$\tau(xy) = \tau(x)\tau(y), \quad x, y \in A.$$

Denote by $ch(A, K)$ the set of all characters of $A$ over $K$.

For each $x \in A$, denote by $\mathrm{gp}_A(x)$ the group generated by $x$ in $A$,

$$\mathrm{gp}_A(x) = \{1, x, \ldots, x^{R-1}\},$$

where the order $R$ of $\mathrm{gp}_A(x)$ is the smallest positive integer satisfying $x^R = 1$. We call $R$ the *order* of $x$.

If $\tau$ is a character of $A$ over $K$ and $x \in A$, then $\tau(x)$ completely determines the values of $\tau$ on $gp_A(x)$ by

$$\tau(x^l) = \tau(x)^l, \quad l \in \mathbf{Z}.$$

In particular, $x^L = 1$ implies $\tau(x)$ is an $L$-th root of unity in $K$.

Denote by $U_N(K)$ the multiplicative group of all $N$-th roots of unity in $K$. The order of $U_N(K)$ divides $N$. Since every $x \in A$ satisfies $x^N = 1$, $\tau(x) \in U_N(K)$, for every character $\tau$ of $A$ over $K$.

*A splits* over $K$ if the number of characters of $A$ over $K$ is the order of $A$. We will eventually show that this is the maximal number of possible characters of $A$ over $K$.

In the following examples $C_N$ is the cyclic group of order $N$ having generator $x$.

**Example 1** There exists $N$ characters of $C_N$ over $\mathbf{C}$ defined by

$$\tau_n(x) = e^{2\pi i \frac{n}{N}}, \quad 0 \le n < N.$$

The multiplicative group $U_N(K)$ is a cyclic subgroup of $K^\times$ whose order $L$ divides $N$. If $\gamma \in U_N(K)$, then $\gamma^L = 1$. The smallest positive power of $\gamma$ equal to 1 is called the order of $\gamma$. Denoting a generator of $U_N(K)$ by $\alpha$, we have that

$$U_N(K) = \{1, \alpha, \ldots, \alpha^{L-1}\}$$

and $\alpha$ has order $L$. We say that $\alpha$ is a *primitive* $N$-th root of unity if the order of $\alpha$ is $N$. $K$ has a primitive $N$-th root of unity if and only if there exists exactly $N$ $N$-th roots of unity in $K$.

$C_N$ splits over $K$ if and only if $K$ has a primitive $N$-th root of unity $\alpha$. The $N$ characters of $C_N$ over $K$ are defined by

$$\tau_n(x) = \alpha^n, \quad 0 \le n < N.$$

**Example 2** cyclotomics

Suppose $K = GF(p^R)$, the field of order $p^R$, $p$ a prime. Since $K^\times$ is a cyclic multiplicative group of order $p^R - 1$, a generator $\alpha$ of $K^\times$ is a primitive $(p^R - 1)$-th root of unity and the order of any power of $\alpha$ must divide $p^R - 1$.

If $N$ divides $p^R - 1$, then

$$\gamma = \alpha^M, \quad p^R - 1 = MN,$$

is a primitive $N$-th root of unity in $K^\times$. We see that $C_N$ splits over $GF(p^R)$ if and only if

$$p^R \equiv 1 \bmod N.$$

In particular, if $C_N$ splits over $GF(p^R)$ then $p$ does not divide $N$.

**Example 3** The finite field $K = GF(27)$ has a primitive 26-th root of unity $\alpha$,

$$K^\times = \{1, \alpha, \ldots, \alpha^{25}\}$$

with $\alpha^{26}$ the smallest positive power of $\alpha$ equal to 1.

**Example 4** Continuing the preceding example, $\alpha^2$ has order 13, $\alpha^{13}$ has order 2 and $\alpha^r$ has order 26 whenever $r$ is relatively prime to 26.

**Example 5** $C_6$ and $C_8$ split over $GF(25)$.

**Example 6** $C_4$ splits over $GF(9)$.

In general, the number of characters of $C_N$ over $K$ is equal to the number of $N$-th roots of unity in $K$. If $U_N(K)$ has order $L$ and $\alpha$ is a generator of $U_N(K)$, the $L$ characters of $C_N$ over $K$ are defined by

$$\tau_l(x) = \alpha^l, \quad 0 \le l < L.$$

If $K$ does not contain a primitive $N$-th root of unity, then the number of characters $L$ of $C_N$ over $K$ is less than $N$. In fact, $L$ is a proper divisor of $N$.

**Example 7** $\mathbf{R}$ has two roots of unity, 1 and $-1$. If $N$ is odd, 1 is the only $N$-th root of unity in $\mathbf{R}$ and $C_N$ has exactly one character over $\mathbf{R}$. If $N$ is even, 1 and $-1$ are the only $N$-th roots of unity in $\mathbf{R}$ and $C_N$ has exactly two characters over $\mathbf{R}$.

**Example 8** $GF(5)$ has exactly two 2-th roots of unity, 1 and 4, and four 4-th roots of unity, 1, 2, 3, 4. There are exactly two 6-th roots of unity 1 and 4, and exactly two characters of $C_6$ over $GF(5)$. There are exactly four 8-th roots of unity, 1, 2, 3, 4 and exactly four characters of $C_8$ over $GF(5)$. In general if $N \equiv 2 \bmod 4$, there are exactly two characters of $C_N$ over $GF(5)$ and if $N \equiv 0 \bmod 4$, there are exactly four characters of $C_N$ over $GF(5)$.

For $K = \mathbf{Q}$ or $K = GF(p^R)$, $p$ a prime not dividing $N$, the condition that $C_N$ splits over $K$ places severe conditions on $N$. One solution is to construct a *minimal* field extension $E$ of $K$ over which $C_N$ splits. $E$ contains $K$ as a subfield, has a primitive $N$-th root of unity and there exists no proper subfield of $E$ containing $K$ having a primitive $N$-th root of unity. There is an elaborate theory for construction such a field extension over an arbitrary field $K$ whose characteristic $p$ does not divide $N$. The resulting field extension $E$ is called the *splitting field* of the polynomial $x^N - 1$ over $K$ and is an example of a *Galois* extension. We will say more about Galois extensions over $\mathbf{Q}$ and $GF(p^R)$ in chapter 4.

For the fields $\mathbf{Q}$ and $GF(p^R)$, the construction of minimal field extensions over which $C_N$ splits is simple and we will restrict our attention to these cases.

For $\mathbf{Q}$, the cyclotomic field $\mathbf{Q}(\xi_N)$, $\xi_N = e^{2\pi i \frac{1}{N}}$, is the minimal field extension of $\mathbf{Q}$ over which $C_N$ splits. For $GF(p^R)$ the construction is slightly more involved. For simplicity we consider the case $GF(p)$, where $p$ does not divide $N$.

Viewing $p$ as an element in $\mathbf{Z}/N$, since $p$ and $N$ are relatively prime, $p$ is in the multiplicative group $U(N)$ of units of $\mathbf{Z}/N$ and some power of $p$ equals 1 mod $N$. The smallest such power $R$, called the order of $p$ in $U(N)$, defines the minimal extension field $GF(p^R)$ over which $C_N$ splits. In general, for any integer $s > 0$, there exists a minimal extensional field of $GF(p^s)$ over which $C_N$ splits.

**Example 9** $GF(25)$ is the minimal extension field of $GF(5)$ over which $C_6$ and $C_8$ splits. $GF(9)$ is the minimal extensional field of $GF(3)$ over which $C_4$ splits.

Consider the direct product $C_{N_1} \times C_{N_2}$ of cyclic groups $C_{N_1}$ and $C_{N_2}$. Denoting generators of $C_{N_1}$ and $C_{N_2}$ by $x_1$ and $x_2$, every element in $C_{N_1} \times C_{N_2}$ can be written uniquely in the form

$$x_1^{n_1} x_2^{n_2}, \quad 0 \leq n_1 < N_1,\ 0 \leq n_2 < N_2.$$

The characters of $C_{N_1} \times C_{N_2}$ over $K$ are completely determined by the characters of $C_{N_1}$ and $C_{N_2}$ over $K$. If $\tau$ is a character of $C_{N_1} \times C_{N_2}$ over $K$, we can define characters $\tau_1$ and $\tau_2$ of $C_{N_1}$ and $C_{N_2}$ over $K$ by

$$\tau_1(x_1) = \tau(x), \quad \tau_2(x_2) = \tau(x_2).$$

$\tau$ is completely determined by $\tau_1$ and $\tau_2$ by

$$\tau(x_1^{n_1} x_2^{n_2}) = \tau_1(x_1)^{n_1} \tau_2(x_2)^{n_2}, \quad 0 \leq n_1 < N_1,\ 0 \leq n_2 < N_2,$$

and we can write $\tau = \tau_1 \otimes \tau_2$. Conversely, if $\tau_1$ and $\tau_2$ are characters of $C_{N_1}$ and $C_{N_2}$ over $K$, then $\tau_1 \otimes \tau_2$ is a character of $C_{N_1} \times C_{N_2}$ over $K$.

$C_{N_1} \times C_{N_2}$ splits over $K$ if and only if $C_{N_1}$ and $C_{N_2}$ split over $K$. This will be the case if and only if $K$ has a primitive $N_1$-th root of unity $\alpha_1$ and a primitive $N_2$-th root of unity $\alpha_2$.

**Example 10** The $N_1N_2$ characters

$$\tau_{\mathbf{n}}, \quad \mathbf{n} = (n_1, n_2),\ 0 \le n_1 < N_1,\ 0 \le n_2 < N_2,$$

of $C_{N_1} \times C_{N_2}$ over $\mathbf{C}$ are defined by

$$\tau_{\mathbf{n}}(x_1^{m_1} x_2^{m_2}) = e^{2\pi i \frac{n_1 m_1}{N_1}} e^{2\pi i \frac{n_2 m_2}{N_2}}, \quad 0 \le m_1 < N_1,\ 0 \le m_2 < N_2.$$

If $K$ has primitive $N_1$-th and $N_2$-th roots of unity $\alpha_1$ and $\alpha_2$, then the $N_1N_2$ characters

$$\tau_{\mathbf{n}}, \quad \mathbf{n} = (n_1, n_2),\ 0 \le n_1 < N_1,\ 0 \le n_2 < N_2,$$

of $C_{N_1} \times C_{N_2}$ over $K$ are defined by

$$\tau_{\mathbf{m}}(x_1^{m_1} x_2^{m_2}) = \alpha_1^{n_1 m_1} \alpha_2^{n_2 m_2}, \quad 0 \le m_1 < N_1,\ 0 \le m_2 < N_2.$$

Denote the least common multiple of $N_1$ and $N_2$ by $[N_1, N_2]$. $\alpha_1\alpha_2$ is a primitive $[N_1, N_2]$-th root of unity. Generally if $K$ has a primitive $[N_1, N_2]$-th root of unity $\alpha$, then

$$\alpha_1 = \alpha^{L_1},\ \alpha_2 = \alpha^{L_2}, \quad [N_1, N_2] = L_1N_1 = L_2N_2$$

are primitive $N_1$-th and $N_2$-th roots of unity in $K$.

$K$ has primitive $N_1$-th and $N_2$-th roots of unity if and only if $K$ has a primitive $[N_1, N_2]$-th root of unity. $C_{N_1} \times C_{N_2}$ *splits* over $K$ if and only if $K$ has a primitive $[N_1, N_2]$-th root of unity.

We ~~can~~ state the condition for $C_{N_1} \times C_{N_2}$ to split over $K$ completely in terms of the abelian group defined by $C_{N_1} \times C_{N_2}$ and not on its representation. Since the order of each element in $C_{N_1}$ divides $N_1$ and the order of each element in $C_{N_2}$ divides $N_2$, $[N_1, N_2]$ is the least common multiple over all orders of elements in $C_{N_1} \times C_{N_2}$.

In general the number of characters of $C_{N_1} \times C_{N_2}$ over $K$ is the product of the number of characters of $C_{N_1}$ over $K$ with the number of characters of $C_{N_2}$ over $K$. This number is equal to $L_1L_2$ where $L_1$ is the number of $N_1$-th roots of unity and $L_2$ is the number of $N_2$-th roots of unity in $K$. If $\alpha_1$ and $\alpha_2$ are generators of $U_{N_1}(K)$ and $U_{N_2}(K)$, the $L_1L_2$ characters of $C_{N_1} \times C_{N_2}$ over $K$

$$\tau_{\mathbf{l}}, \quad \mathbf{l} = (l_1, l_2),\ 0 \le l_1 < L_1,\ 0 \le l_2 < L_2,$$

are given by

$$\tau_{\mathbf{l}}(x_1^{m_1} x_2^{m_2}) = \alpha_1^{l_1 m_1} \alpha_2^{l_2 m_2}, \quad 0 \le m_1 < N_1,\ 0 \le m_2 < N_2.$$

The results of this section easily extend to an arbitrary finite number of cyclic groups

$$A = C_{N_1} \times \cdots \times C_{N_R}.$$

Each character $\tau$ of $A$ over $K$ is uniquely represented by

$$\tau = \tau_1 \otimes \cdots \otimes \tau_R,$$

where $\tau_r$ is a character of $C_{N_r}$ over $K$, $1 \le r \le R$. $A$ splits over $K$ if and only if $C_{N_r}$ splits over $K$, $1 \le r \le R$ and in general the number of characters of $A$ over $K$ is equal to $L = L_1 \cdots L_R$, where $L_r$ is the number of characters of $C_{N_r}$ over $K$, $1 \le r \le R$. Since every finite abelian group $A$ is the product of a finite number of finite cyclic groups, this completes the description of $Ch(A : K)$ for every finite abelian group $A$ and field $K$.

# 4 Group algebra of $A$

The group algebra $KA$ of $A$ over $K$ is the $K$-vector space of all formal sums

$$f = \sum_{x \in A} f(x)x, \qquad f(x) \in K,$$

under

$$f + g = \sum_{x \in A} (f(x) + g(x))\, x, \qquad f, g \in KA,$$

$$\alpha f = \sum_{x \in A} (\alpha f(x))\, x, \qquad \alpha \in K, f \in KA,$$

with $K$-algebra multiplication

$$fg = \sum_{y \in A} \left( \sum_{x \in A} f(x) g(x^{-1}y) \right) y, \qquad f, g \in KA.$$

The additions and multiplications inside the brackets are taken in $K$. Since $A$ is abelian, the $K$-algebra multiplication is commutative.

Denote by $L(A; K)$, the $K$-vector space of all $K$-valued functions on $A$. Every $f \in L(A : K)$ defines a formal sum in $KA$

$$f = \sum_{x \in A} f(x)x$$

and we can identify the $K$-vector space $KA$ with the $K$-vector space $L(A; K)$. The multiplication $f \cdot g$ in $KA$ corresponds to the standard convolution in $L(A; K)$

$$f * g(y) = \sum_{x \in A} f(x) g(x^{-1}y), \qquad y \in A,\ f, g \in L(A; K).$$

Under this identification the delta function $\delta_y$, $y \in A$ corresponds to the formal sum in $KA$

$$\sum_{x \in A} \delta_y(x)x$$

which we denote by $y$. In this way, we can view $A$ as a subset of $KA$. $A$ is a basis of the $K$-vector space $KA$ and $KA$ has dimension $N$, the order of $A$. The identity 1 in $A$ is the identity of the $K$-algebra $KA$.

We will usually use the term basis for any subset of vector space which if ordered is a basis in the usual sense. In summation expressions, there is no loss in doing so. However whenever matrices are involved, an ordering must be specified even if implicitly.

For $y \in A$ and $f \in KA$

$$yf = \sum_{x \in A} f(x)yx = \sum_{x \in A} f(y^{-1}x)x.$$

We call $yf$ the translation of $f$ by $y$. The term $f(y^{-1}x)$ in the right-hand summation identifies $yf$ with the usual definition of translation in engineering terminology. For $y \in A$, the operator $L(y)$ of $KA$ defined by

$$L(y)f = yf, \qquad f \in KA,$$

is a linear isomorphism of the $K$-vector space $KA$ and we have

$$L(zy) = L(z)L(y), \qquad z, y \in A$$
$$L(z^{-1}) = L(z)^{-1}, \qquad z \in A$$

where $L(z)L(y)$ and $L(z)^{-1}$ denote composition and inversion of operators in $KA$. Observe that for every $y \in A$, $L(y)$ acts as a permutation on the basis $A$ of $KA$.

**Example 11** Ordering $C_4$ by successive powers of a generator $x$,

$$1, x, x^2, x^3,$$

the matrix of $L(x^m)$ relative to the resulting basis $C_4$ of $KC_4$ is $S_4^m$, $0 \le m < 4$, where $S_4$ is the 4-point cyclic shift matrix.

In general, ordering $C_N$ by successive powers of a generator $x$, the matrix of $L(x^m)$ relative to the resulting basis $C_N$ of $KC_N$ is $S_N^m$, $0 \le m < N$, where $S_N$ is the $N$-point cyclic shift matrix.

**Example 12** Ordering $C_4 \times C_3$ by first ordering $C_4$ and $C_3$ by successive powers of generators $x_1$ and $x_2$ and then by imposing the lexicographic ordering on $C_4 \times C_3$

$$1,\ x_2,\ x_2^2;\ x_1,\ x_1x_2,\ x_1x_2^2;\ x_1^2,\ x_1^2x_2,\ x_1^2x_2^2;\ x_1^3,\ x_1^3x_2,\ x_1^3x_2^2,$$

the matrix of $L(x_1^{m_1}x_2^{m_2})$ relative to the resulting basis $C_4 \times C_3$ of $K(C_4 \times C_3)$ is $S_4^{m_1} \otimes S_3^{m_2}$, $0 \le m_1 < 4$, $0 \le m_2 < 3$.

In general ordering the direct product

$$C_{N_1} \times \cdots \times C_{N_R}$$

by first ordering the factors $C_{N_r}$ by successive powers of generators $x_r$, $1 \leq r \leq R$, and then by imposing the lexicographic ordering on the direct product, the matrix of

$$L(x_1^{m_1} \cdots x_R^{m_R})$$

relative to the resulting basis $C_{N_1} \times \cdots \times C_{N_R}$ of $K(C_{N_1} \times \cdots \times C_{N_R})$ is

$$S_{N_1}^{m_1} \otimes \cdots \otimes S_{N_R}^{m_R}.$$

Denote by $GL(KA; K)$ the group of linear isomorphisms of the $K$-vector space $KA$. The mapping

$$L : A \to GL(KA; K)$$

is an isomorphism of the group $A$ into the group $GL(KA, K)$. We say that $L$ is a representation of $A$ on $KA$ and call $L$ the regular representation of $A$.

A subspace $V$ of the $K$-vector space $KA$ is called *$A$-invariant* if for each $y \in A$

$$yV = \{yf : f \in V\} \subset V.$$

If $V$ is $A$-invariant and $f(x)$, $x \in A$, is a coefficient set for a formal sum in $V$, then for each $y \in A$, $f(y^{-1}x)$, $x \in A$, is also a coefficient set for a formal sum in $V$. $A$-invariant subspaces of $KA$ can be identified with translation-invariant subspaces of $K$-valued functions of $A$.

**Example 13** The subspace of $KA$ spanned by the formal sum

$$\sum_{x \in A} 1x$$

is the $A$-invariant subspace of $KA$ consisting of all formal sums in $KA$ unchanged by the action of the operators $L(y)$, $y \in A$.

For a subgroup $B$ of $A$, we say that a subspace $V$ of the $K$-vector space $KA$ is $B$-invariant if for all $y \in B$,

$$yV \subset V.$$

The $B$-invariant subspace of $KA$

$$\{f \in KA : yf = f, \text{ for all } y \in B\}$$

can be identified with the subspace of $B$-periodic $K$-valued functions on $A$.

For $g \in KA$ define the operator $L(g)$ of $KA$ by

$$L(g)f = gf, \quad f \in KA.$$

Since

$$L(g)f = gf = \sum_{y \in A} g(y)(yf) = \sum_{y \in A} g(y)L(y)f = \left( \sum_{y \in A} g(y)L(y) \right) f$$

we have that

$$L(g) = \sum_{y \in A} g(y)L(y)$$

linearly extends the domain of definition of $L$ from $A$ to $KA$. In particular, the two definitions coincide on $A$.

$L(g)$, $g \in KA$, is a homomorphism of the $K$-vector space $KA$ but is not necessarily an isomorphism as is the case with $L(y)$, $y \in A$. We can have $gf = 0$ for $f, g \in KA$ with both $f$ and $g$ not zero.

**Example 14** Continuing example 11, the matrix of $L(g)$ $g \in K(C_4)$, relative to the basis $C_4$ is

$$C_4(g) = \sum_{m=0}^{3} g(x^m) S_4^m.$$

Defining $\mathbf{g} \in K^4$ by

$$\mathbf{g} = [g(x^m)]_{0 \le m < 4}$$

we have

$$C_4(g) = \left[ \begin{array}{cccc} \mathbf{g} & S_4\mathbf{g} & S_4^2\mathbf{g} & S_4^3\mathbf{g} \end{array} \right].$$

If we take $g = \sum_{y \in C_4} y$, then $C_4(g)$ is the singular $4 \times 4$ matrix of all ones.

In general, ordering $C_N$ by successive powers of a generator $x$, the matrix of $L(g)$, $g \in KC_N$, relative to the resulting basis $C_N$ is

$$C_N(g) = \sum_{m=0}^{N-1} g(x^m) S_N^m.$$

Defining $\mathbf{g} \in K^N$ by

$$\mathbf{g} = [g(x^m)]_{0 \le m < N},$$

we have

$$C_N(g) = \left[ \begin{array}{cccc} \mathbf{g} & S_N\mathbf{g} & \cdots & S_N^{N-1}\mathbf{g} \end{array} \right].$$

Linear combinations over $K$ of powers of $S_N$ are called $N$-point *circulant* matrices over $K$. Such matrices are completely determined by their 0-th column.

$C_N$ can be realized relative to the basis $C_N$ as the matrix product of the circulant matrix $C_N(g)$ with the vector $\mathbf{f}$ formed by ordering the values of $f$ according to successive powers of the generator.

**Example 15** Continuing example 14, for $f$ and $g$ in $KC_4$, the product $h = fg$ is given by

$$\mathbf{h} = C_4(g)\mathbf{f}.$$

**Example 16** Continuing example 12, the matrix of $L(g)$, $g \in K(C_4 \times C_3)$ relative to the basis $C_4 \times C_3$ is

$$\sum_{m_1=0}^{3} \sum_{m_2=0}^{2} g(x_1^{m_1} x_2^{m_2}) x_1^{m_1} x_2^{m_2}.$$

Denote by $C(m)$ the $3 \times 3$ circulant matrix having 0-th column

$$\begin{bmatrix} g(x_1^m) \\ g(x_1^m x_2) \\ g(x_1^m x_2^2) \end{bmatrix}, \quad 0 \leq m < 4.$$

The matrix of $L(g)$ can be written as

$$\begin{bmatrix} c(0) & c(3) & c(2) & c(1) \\ c(1) & c(0) & c(3) & c(2) \\ c(2) & c(1) & c(0) & c(3) \\ c(3) & c(2) & c(1) & c(0) \end{bmatrix}$$

which is an example of a *block-circulant matrix having circulant blocks.*

Denote by $gl(KA; K)$ the $K$-algebra of all homomorphisms of the $K$-vector space $KA$. The mapping

$$L : KA \to gl(KA; K)$$

is a $K$-algebra isomorphism of $KA$ into $gl(KA; K)$.

For an $A$-invariant subspace $V$ of $KA$ and $f \in V$, we have for all $g \in KA$,

$$L(g)f = \sum_{y \in A} g(y)L(y)f \in V$$

and $V$ is $KA$-invariant. The equivalence of $A$-invariance and $KA$-invariance will be used throughout this work.

A homomorphism $T$ of the $K$-vector space $KA$ is called *$A$-invariant* if for all $y \in A$,

$$L(y)T = TL(y).$$

**Example 17** $L(g)$, $g \in KA$ is $A$-invariant.

In fact, the operators $L(g)$, $g \in KA$ are the only $A$-invariant homomorphisms of $KA$. For an $A$-invariant $T$ and $f \in KA$

$$yT(f) = T(yf), \quad y \in A.$$

In particular, with $f = 1$ in $KA$,

$$T(y) = T(1)y$$

and

$$T(f) = \sum_{y \in A} f(y)T(y) = T(1) \sum_{y \in A} f(y)y = T(1)f.$$

The claim is proved since

$$T = L(g), \quad g = T(1).$$

# 5 Fourier transform over $A$

Decompositions of $KA$ into direct sums of $A$-invariant subspaces play two important roles: algorithm design for computing products in $KA$ and spectral analysis. The Fourier transform over $A$ is the simplest and most frequently occurring example.

A character $\tau$ of $A$ over $K$ determines the formal sum in $KA$

$$\tau = \sum_{x \in A} \tau(x)x.$$

Multiplication of characters will always be taken in $KA$ with the warning that in many places, another multiplication is defined under which $\mathrm{ch}(A; K)$ is a group. The importance of characters in studying $A$-invariant subspaces of $KA$ is contained in the following result.

**Theorem 1** *For $f \in KA$ and $\tau$ a character of $A$ over $K$,*

$$f\tau = \hat{f}(\tau)\tau,$$

*where $\hat{f}(\tau) \in K$ is given by*

$$\hat{f}(\tau) = \sum_{y \in A} f(y)\tau(y^{-1}).$$

**Proof** For $y \in A$

$$\begin{aligned} y\tau &= \sum_{x \in A} \tau(x)yx = \sum_{x \in A} \tau(y^{-1}x)x = \tau(y^{-1}) \sum_{x \in A} \tau(x)x \\ &= \tau(y^{-1})\tau. \end{aligned}$$

The theorem follows from

$$f\tau = \sum_{y\in A} f(y)(y\tau) = \left(\sum_{y\in A} f(y)\tau(y^{-1})\right)\tau.$$

For two characters $\tau$ and $\lambda$ of $A$ over $K$, since $\tau\lambda = \lambda\tau$, we have

$$\tau\lambda = \alpha\lambda = \alpha\tau = \lambda\tau,$$

where $\alpha = \hat{\tau}(\lambda) = \hat{\lambda}(\tau)$. If $\tau \neq \lambda$, then $\alpha = 0$ and $\tau\lambda = 0$. If $\tau = \lambda$, then

$$\alpha = \sum_{y\in A} \tau(y)\tau(y^{-1}) = \sum_{y\in A} 1 = N$$

and $\tau^2 = N\tau$, proving the following.

**Corollary 1** *For two characters $\tau$ and $\lambda$ of $A$ over $K$,*

$$\tau\lambda = \begin{cases} N\tau, & \tau = \lambda, \\ 0, & \tau \neq \lambda. \end{cases}$$

In the following discussion, we abbreviate $\mathrm{ch}(A;K)$ by $A^*$ and view $A^*$ as a subset of $KA$.

**Corollary 2** *$A^*$ is a linearly independent subset in the $K$-vector space $KA$.*

**Proof** Suppose

$$0 = \sum_{\tau\in A^*} \alpha(\tau)\tau, \qquad \alpha(\tau) \in K.$$

By corollary 1, for any $\lambda \in A^*$

$$\lambda \sum_{\tau\in A^*} \alpha(\tau)\tau = N\alpha(\lambda)\lambda = 0$$

and $\alpha(\lambda) = 0$. Since this holds for any $\lambda \in A^*$, the corollary follows.

By the theorem, the $K$-subspace spanned by a character $\tau$ over $K$ is $A$-invariant

$$KA\tau = K\tau.$$

By corollary 2, we have the direct sum of one-dimensional $A$-invariant subspaces of $KA$,

$$\sum_{\tau\in A^*} \oplus K\tau.$$

## 5.1 Split case

Suppose $A$ splits over $K$. By corollary 2, $A^*$ is a basis of the $K$-vector space $KA$ and we have the following result.

**Theorem 2** *$KA$ is the direct sum of one-dimensional $A$-invariant subspaces*

$$KA = \sum_{\tau \in A^*} \oplus K\tau.$$

By theorem 2,

$$1 = \sum_{\tau \in A^*} \alpha(\tau)\tau, \qquad \alpha(\tau) \in K.$$

For any $\lambda \in A^*$,

$$\lambda = \lambda \cdot 1 = \sum_{\tau \in A^*} \alpha(\tau)\lambda\tau = N\alpha(\lambda)\lambda$$

and $\alpha(\lambda) = \frac{1}{N}$, proving the following.

**Corollary 3**

$$1 = \frac{1}{N} \sum_{\tau \in A^*} \tau.$$

By corollary 3,

$$f = \frac{1}{N} \sum_{\tau \in A^*} f\tau = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\tau$$

is the expansion of $f$ over the basis $A^*$ of $KA$. The coefficient set of this expansion (up to scale multiple $\frac{1}{N}$)

$$\hat{f}(\tau), \qquad \tau \in A^*,$$

is called the *Fourier transform* of $f$ in $KA$. By theorem 1,

$$\hat{f}(\tau) = \sum_{y \in A} f(y)\tau(y^{-1}).$$

The linear isomorphism that maps the coefficient set of the expansion of $f$ over the basis $A$

$$f(x), \qquad x \in A,$$

onto the coefficient set of the expansion of $f$ over the basis $A^*$ (up to scale multiple $\frac{1}{N}$)

$$\hat{f}(\tau), \qquad \tau \in A^*$$

is called the *Fourier transform* over $KA$. The inversion that maps coefficient sets over $A^*$ onto coefficient sets over $A$

$$f(x) = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\tau(x), \qquad x \in A,$$

is called the *inverse Fourier transform* over $KA$.

**Example 18** Examples

The basis $A^*$ of $KA$ is a *diagonalizing basis* for the operators $L(g)$, $g \in KA$, since

$$L(g)\tau = g\tau = \hat{g}(\tau)\tau, \qquad \tau \in A^*$$

and a diagonalizing basis for multiplication in $KA$.

**Theorem 3** *For $f$ and $g$ in $KA$,*

$$fg = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\hat{g}(\tau)\tau.$$

**Proof**

$$\begin{aligned} fg &= \frac{1}{N^2} \left( \sum_{\tau \in A^*} \hat{f}(\tau)\tau \right) \left( \sum_{\lambda \in A^*} \hat{g}(\lambda)\lambda \right) \\ &= \frac{1}{N^2} \sum_{\tau \in A^*} \sum_{\lambda \in A^*} \hat{f}(\tau)\hat{g}(\lambda)\tau\lambda \\ &= \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\hat{g}(\tau)\tau, \end{aligned}$$

completing the proof.

**Corollary 4** *If $f \in KA$ satisfies $f^2 = 0$, then $f = 0$.*

**Proof** By theorem 3

$$f^2 = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)^2\tau = 0$$

implying, since $A^*$ is a basis of $KA$, that

$$\hat{f}(\tau) = 0, \qquad \tau \in A^*,$$

and $f = 0$ proving the corollary.

The theorem leads to an algorithm for computing $fg$, $f, g \in KA$.

- Compute the Fourier transform

$$\hat{f}(\tau), \quad \tau \in A^*.$$

- Compute the Fourier transform

$$\hat{g}(\tau), \quad \tau \in A^*.$$

- Compute the product in $K$

$$\hat{f}(\tau)\hat{g}(\tau), \quad \tau \in A^*.$$

- Compute the inverse Fourier transform of these products

$$fg.$$

The importance of this algorithm to compute $fg$, $f$, $g \in KA$, based on the existence of fast algorithms to compute the Fourier transform.

An $A$-invariant subspace $W$ of $KA$ is called *irreducible* if the only $A$-invariant subspaces of $W$ are (0) and $W$. For $\tau \in A^*$, $K\tau$ is an irreducible $A$-invariant subspace of $KA$. In the split case the $A$-invariant and irreducible $A$-invariant subspaces of $KA$ can be completely described in terms of the subspaces $K\tau$, $\tau \in A^*$.

**Theorem 4** *If $W$ is an $A$-invariant subspace of $KA$, then*

$$W = \sum_{\tau \in \Delta} \oplus K\tau = KAe,$$

*where $\Delta = W \cap A^*$ and $e = \frac{1}{N}\sum_{\tau \in \Delta} \tau$.*

**Proof** For $f \in W$ and $\lambda \in A^*$

$$\lambda f = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\lambda\tau = \frac{1}{N}\hat{f}(\lambda)\lambda.$$

Since $W$ is $A$-invariant,

$$\hat{f}(\lambda)\lambda \in W, \quad \lambda \in A^*.$$

If $\hat{f}(\lambda) \neq 0$, then $\lambda \in W$ proving that every $f \in W$ is contained in the $K$-linear span of the set of characters contained in $W$, proving $W = \sum_{\tau \in \Delta} \oplus K\tau$.

Since $e \in W$ and $W$ is $A$-invariant, $KAe \subset W$. For any $\lambda \in \Delta$, $\lambda e = \frac{1}{N}\lambda \in KAe$, proving $W \subset KAe$, completing the proof of the theorem.

The factor $\frac{1}{N}$ in the definition of $e$ has been chosen so that $e^2 = e$, the relevance of which will be made clear in the next section.

If $W$ is an irreducible $A$-invariant subspace of $KA$, then by theorem 4, $W$ contains a unique $\tau \in A^*$ and $W = K\tau$, proving the following corollary.

**Corollary 5** *The irreducible $A$-invariant subspaces of $KA$ are given by $K\tau$, $\tau \in A^*$.*

Denote the complement of $\Delta = W \cap A^*$ in $A^*$ by $\Delta^c$. By theorem 2 and theorem 4, we have the following result.

**Corollary 6** *$KA$ is the direct sum of $A$-invariant subspaces,*

$$KA = W \oplus W',$$

*where*

$$W' = \sum_{\tau \in \Delta^c} \oplus K\tau = KAe',$$

*and $e' = \frac{1}{N} \sum_{\tau \in \Delta^c} \tau$.*

The $A$-invariant subspace $W$ of $KA$ in theorem 4 can also be described by

$$W = \{f \in KA : \hat{f}(\tau) = 0, \text{ for all } \tau \in \Delta^c\}. \tag{1}$$

In general, if $\Delta$ is an arbitrary subset of $A^*$ and $\Delta^c$ its complement in $A^*$, the subspace of $KA$ define in ( 1) is $A$-invariant. This follows from the diagonalizing formula for the Fourier transform and the nonvanishing of characters.

By the results just described, single characters determine irreducible $A$-invariant subspaces, collections of characters determine $A$-invariant subspaces and partitions of the collection of all characters determine direct sum decompositions of $KA$ into $A$-invariant subspaces.

## 5.2 Nonsplit case

If $A$ does not split over $K$, then $KA$ does not decompose into the direct sum of *one-dimensional* $A$-invariant subspaces, but does have decompositions into the direct sum of irreducible $A$-invariant subspaces. For $K = \mathbf{Q}$ or $K = GF(p^R)$, $p$ a prime not dividing $N$, we have constructed a minimal field extension of $K$ over which $C_N$ splits or equivalently, having a primitive $N$-th root of unity. If $N$ is the least common multiple of the orders of the elements in $A$, then the same construction produces a minimal field extension $E$ of $K$ over which $A$ splits. We call $E$ the *splitting field* of $A$ over $K$.

We will show how splitting fields of $A$ over $K$ can be used to construct decompositions of $KA$ into direct sums of irreducible $A$-invariant subspaces. The irreducible $A$-invariant spaces will not generally be one-dimensional. The first new concept required is that of idempotents which replace characters as the structural basis of these decompositions.

Suppose $A$ is a finite abelian group of order $N$ and $K$ is a field over which $A$ does not necessarily split. We assume throughout that $K = \mathbf{Q}$ or $K = GF(p^R)$ where $p$ does not divide $N$.

A nonzero element $e \in KA$ is called an *idempotent* if $e^2 = e$. Two idempotents $e_1$ and $e_2$ are said to be *orthogonal* if $e_1 e_2 = e_2 e_1 = 0$. A set of pairwise orthogonal idempotents

$$\{e_1, \ldots, e_J\}$$

is called a *complete set of orthogonal idempotents* if

$$1 = \sum_{j=1}^{J} e_j.$$

The sum of orthogonal idempotents $e_1$ and $e_2$ is an idempotent since

$$(e_1 + e_2)^2 = e_1^2 + e_1 e_2 + e_2 e_1 + e_2^2 = e_1 + e_2,$$

and if $e$ is an idempotent, the set

$$\{e, 1 - e\}$$

is a complete set of orthogonal idempotents.

**Example 19** If $\tau$ is a character of $A$ over $K$, then by corollary 1,

$$e = \frac{1}{N}\tau$$

is an idempotent of $KA$. If $\tau_1$ and $\tau_2$ are characters of $A$ over $K$, then the corresponding idempotents $e_1 = \frac{1}{N}\tau_1$ and $e_2 = \frac{1}{N}\tau_2$ are orthogonal.

**Example 20** Suppose $A$ splits over $K$. Denote the set of all characters of $A$ over $K$ by $A^*$. By corollary 3, the set of idempotents

$$\{e = \frac{1}{N}\tau : \tau \in A^*\}$$

is a complete set of orthogonal idempotents of KA.

A complete set of orthogonal idempotents can be used to decompose $KA$ into a direct sum of $A$-invariant subspaces in much the same way as, in the split case, the set of characters produce such a decomposition. However, the $A$-invariant subspaces generated by the idempotents will not generally be one-dimensional or even be irreducible.

**Theorem 5** *If*

$$\{e_j : 1 \leq j \leq J\}$$

*is a complete set of orthogonal idempotents, then $KA$ is the direct sum of $A$-invariant subspaces*

$$KA = \sum_{j=1}^{J} \oplus KAe_j.$$

**Proof** Define

$$W_j = KAe_j, \quad 1 \leq j \leq J.$$

$W_j$ is the $A$-invariant subspace of $KA$ generated by $e_j$. Consider the sum $\sum_{j=1}^{J} W_j$. By orthogonality, if

$$0 = \sum_{j=1}^{J} f_j e_j, \quad f_j \in KA,$$

then

$$0 = e_k \cdot 0 = f_k e_k, \quad 1 \leq k \leq J,$$

and the sum is a direct sum $\sum_{j+1}^{J} \oplus W_j$. The completeness condition, $1 = \sum_{j=1}^{J} e_j$, implies that for every $f \in KA$,

$$f = \sum_{j=1}^{J} f e_j \in \sum_{j=1}^{J} \oplus W_j,$$

proving the theorem.

The $A$-invariant subspaces $KAe_j$, $1 \leq j \leq J$, in theorem 5 are not necessarily irreducible. In order to derive conditions on and eventually construct sets of orthogonal idempotents producing decompositions into irreducible $A$-invariant subspaces, we will use the splitting field $E$ of $A$ over $K$ and the *Galois group* of the corresponding extension of $E$ over $K$.

Suppose that $E$ is the splitting field for $A$ over $K$. A mapping $\sigma : E \rightarrow E$ is called an *automorphism* of $E$ *over* $K$ is $\sigma$ is an automorphism of the field $E$ fixing the elements in $K$. The collection of all automorphisms of $E$ over $K$ forms a group under composition called the *Galois group* of $E$ over $K$.

Denote by $\Gamma$ the Galois group of $E$ over $K$. The order of $\Gamma$ equals the dimension of $E$ as a $K$-vector space.

The main result we require from Galois theory is the following.

**Theorem 6** *If $\alpha \in E$ satisfies, for all $\sigma \in \Gamma$,*

$$\sigma(\alpha) = \alpha,$$

*then $\alpha \in K$.*

Suppose that $\phi(N)$ is the order of the group of units $U(N)$ of $\mathbf{Z}/N$.

**Example 21** The cyclotomic field $\mathbf{Q}(\xi_n)$, $\xi_n = e^{2\pi i \frac{1}{N}}$, is the minimal extension of $\mathbf{Q}$ over which $C_N$ splits. $\mathbf{Q}(\xi_N)$ has dimension $\phi(N)$ as a vector space over $\mathbf{Q}$. The Galois group of the extension is isomorphic to $U(N)$ having elements uniquely defined by

$$\sigma(\xi_N) = \xi_N^n, \quad n \in U(N).$$

**Example 22** For a prime $p$ not dividing $N$ and $R$ the smallest positive integer satisfying $p^R \equiv 1 \bmod N$, $GF(p^R)$ is the splitting field of $C_N$ over $GF(p)$. $GF(p^R)$ has dimension $R$ as a vector space over $GF(p)$. The Galois group of the extension is isomorphic to the cyclic group $C_R$ and is generated by the automorphism defined by

$$\sigma(\alpha) = \alpha^p, \quad \alpha \in GF(p^R).$$

$\Gamma$ acts on $EA$ and on $A^* = \mathrm{ch}(A, E)$. For $f \in EA$ and $\sigma \in \Gamma$, define $f^\sigma \in EA$ by

$$f^\sigma = \sum_{x \in A} \sigma(f(x))x.$$

If $\sigma_1$, $\sigma_2 \in \Gamma$, then $f^{\sigma_1\sigma_2} = (f^{\sigma_2})^{\sigma_1}$. As a corollary to theorem 6, we have the following.

**Corollary 7** *For $f \in EA$, $f^\sigma = f$, for all $\sigma \in \Gamma$, if and only if $f \in KA$.*

For $\tau \in A^*$, $\tau^\sigma \in A^*$, for all $\sigma \in \Gamma$. Define

$$\Gamma\tau = \{\tau^\sigma : \sigma \in \Gamma\}$$

and call $\Gamma\tau$ the $\Gamma$-*orbit* at $\tau$. If $\tau' \in \Gamma\tau$, then $\Gamma\tau = \Gamma\tau'$ and if $\Gamma\tau_1 \cap \Gamma\tau_2$ is not empty for $\tau_1$, $\tau_2 \in A^*$, then $\Gamma\tau_1 = \Gamma\tau_2$. The action of $\Gamma$ on $A^*$ partitions $A^*$ into the disjoint union of $\Gamma$-orbits.

A subset $\Delta$ of $A^*$ is called $\Gamma$-*invariant* if $\tau \in \Delta$ implies $\tau^\sigma \in \Delta$, for all $\sigma \in \Gamma$. A $\Gamma$-invariant subset $\Delta$ of $A^*$ is the disjoint union of the $\Gamma$-orbits contained $\Delta$.

We will see that the $\Gamma$-invariant subsets of $A^*$ determine the $A$-invariant subspaces of $KA$ and that the $\Gamma$-orbits in $A^*$ determine the irreducible $A$-invariant subspaces of $KA$. Moreover, we will show the relationship between decompositions of $\Gamma$-invariant subsets of $A^*$ into disjoint unions of $\Gamma$-invariant subsets and decompositions of $A$-invariant subspaces of $KA$ into direct sums of $A$-invariant subspaces.

For $\tau \in A^*$, define $e_\tau \in EA$ by

$$e_\tau = \frac{1}{N} \sum_{\tau' \in \Gamma\tau} \tau'.$$

If $\lambda \in \Gamma\tau$, then $e_\lambda = e_\tau$ and $e_\tau$ depends solely on the $\Gamma$-orbit at $\tau$.

**Theorem 7** *For $\tau \in A^*$, $e_\tau$ is an idempotent in $KA$.*

**Proof** By corollary 1, $e_\tau^2 = e_\tau$. Since $\tau' \in \Gamma\tau$ if and only if $(\tau')^\sigma \in \Gamma\tau$ for all $\sigma \in \Gamma$, we have

$$e_\tau^\sigma = e_\tau, \quad \sigma \in \Gamma,$$

which by corollary 7 implies $e_\tau \in KA$ completing the proof.

Theorem 7 provides a method for constructing idempotents in $KA$ from $\Gamma$-orbits of characters in $A^*$. Moreover, if $\tau_1, \tau_2 \in A^*$ lie on distinct $\Gamma$-orbits, then by corollary 1

$$e_{\tau_1} e_{\tau_2} = 0,$$

and the idempotents $e_{\tau_1}$ and $e_{\tau_2}$ are orthogonal. Each $\Gamma$-orbit determines an idempotent and distinct $\Gamma$-orbits determine distinct orthogonal idempotents.

Denote by $A^*/\Gamma$ any complete set of representatives of $\Gamma$-orbits in $A^*$. $A^*/\Gamma$ is a set formed by choosing a single character in each $\Gamma$-orbit. If $\Delta$ is a $\Gamma$-invariant subset of $A^*$, denote by $\Delta/\Gamma$ the subset of $A^*/\Gamma$ formed by the characters contained in $\Delta$.

**Theorem 8** *The set*

$$\{e_\tau : \tau \in A^*/\Gamma\}$$

*is a complete set of orthogonal idempotents in $KA$.*

**Proof** The proof follows from corollary 3 and

$$\sum_{\tau \in A^*/\Gamma} e_\tau = \frac{1}{N} \sum_{\tau \in A^*} \tau.$$

We will see eventually that the set of idempotents in theorem 8 is special in the sense that the $A$-invariant subspace generated by $e_\tau$, $KAe_\tau$, is an irreducible $A$-invariant subspace in $KA$.

For any $\Gamma$-invariant subset $\Delta$ of $A^*$, define

$$e_\Delta = \frac{1}{N} \sum_{\tau \in \Delta} \tau.$$

Since $\Delta$ is $\Gamma$-invariant, it is the disjoint union of $\Gamma$-orbits and we can write $e_\Delta$ as a sum of orthogonal idempotents

$$e_\Delta = \sum_{\tau \in \Delta/\Gamma} e_\tau,$$

proving the following result.

**Theorem 9** *For any $\Gamma$-invariant subset $\Delta$ of $A^*$,*

$$e_\Delta = \frac{1}{N} \sum_{\tau \in \Delta} \tau$$

*is an idempotent in $KA$ and*

$$KAe_\Delta = \sum_{\tau \in \Delta/\Gamma} \oplus KAe_\tau.$$

$\Gamma$-invariant subsets of $A$ define idempotents in $KA$ and as we will see below every idempotent in $KA$ comes from a $\Gamma$-invariant subset by the formula in theorem 9.

**Corollary 8** *If $\Delta_1$ and $\Delta_2$ are nonintersecting $\Gamma$-invariant subsets of $A^*$, then $e_{\Delta_1}$ and $e_{\Delta_2}$ are orthogonal idempotents in $KA$.*

**Corollary 9** *If $\Delta$ is a $\Gamma$-invariant subset and $\Delta^c$ is its complement in $A^*$, then $\Delta^c$ is $\Gamma$-invariant and*

$$\{e_\Delta, e_{\Delta^c}\}$$

*is a complete system of orthogonal idempotents in $KA$.*

More generally if $A^*$ is the disjoint union of $\Gamma$-invariant subsets $A^* = \cup_{r=1}^{R} \Delta_R$, then the set

$$\{e_{\Delta_r} : 1 \leq r \leq R\}$$

is a complete set of orthogonal idempotents of $KA$. By theorem 5, $KA$ is the direct sum decomposition of the $A$-invariant subspaces

$$KA = \sum_{r=1}^{R} \oplus KAe_{\Delta_r}.$$

**Corollary 10** *For $\Gamma$-invariant subsets $\Delta_1$ and $\Delta_2$ of $A^*$, $\Delta_1 \subset \Delta_2$ if and only if $KAe_{\Delta_1} \subset KAe_{\Delta_2}$.*

**Proof** If $\Delta_1 \subset \Delta_2$, then $KAe_{\Delta_1} \subset KAe_{\Delta_2}$ by theorem 9. Conversely, if $KAe_{\Delta_1} \subset KAe_{\Delta_2}$, we can write

$$e_{\Delta_1} = fe_{\Delta_2}, \quad f \in KA.$$

For any $\tau \in \Delta_1$,

$$\tau = \tau e_{\Delta_1} = f\tau e_{\Delta_2}$$

which since $\tau \neq 0$ implies $\tau \in \Delta_2$ completing the proof.

**Theorem 10** *If $e$ is an idempotent in $KA$, there exists a unique $\Gamma$-invariant subset $\Delta$ of $A^*$ such that $e = e_\Delta$.*

**Proof** Since $e \in EA$, we can write

$$e = \frac{1}{N} \sum_{\tau \in A^*} \hat{e}(\tau)\tau.$$

The idempotent condition $e^2 = e$ implies

$$\hat{e}(\tau)^2 = \hat{e}(\tau), \quad \tau \in A^*,$$

and $\hat{e}(\tau)$ is either 0 or 1. Denote by $\Delta$ the set of all $\tau \in A^*$ such that $\hat{e}(\tau) = 1$. Since $e^\sigma = e$, for all $\sigma \in \Gamma$, $\Delta$ is $\Gamma$-invariant and $e = e_\Delta$, proving the theorem.

Suppose $W$ is an $A$-invariant subspace of $KA$ and $W_E$ is the $E$-subspace spanned by $W$ in $EA$. $W_E$ is an $A$-invariant subspace of $EA$. If

$$\{w_r : 1 \leq r \leq R\}$$

is a basis of the $K$-vector space $W$, it is also a basis of the $E$-vector space $W_E$ and $W = W_E \cap KA$.

**Theorem 11** *$W_E$ is $\Gamma$-invariant. If $f \in W_E$, then $f^\sigma \in W_E$, for all $\sigma \in \Gamma$.*

**Proof** If $f \in W_E$, then

$$f = \sum_{r=1}^{R} \alpha(r) w_r, \qquad \alpha(r) \in E,$$

and for all $\sigma \in \Gamma$,

$$f^\sigma = \sum_{r=1}^{R} \alpha(r)^\sigma w_r \in W_E,$$

proving the theorem.

Set $\Delta = W_E \cap A^*$ and denote the complement of $\Delta$ in $A^*$ by $\Delta^c$. Theorem 11 implies $\Delta$ and $\Delta^c$ are $\Gamma$-invariant. By theorem 4 especially the decomposition of $W_E$ given in ( 1), we have

$$W = \{f \in KA : \hat{f}(\tau) = 0, \text{ for all } \tau \in \Delta^c\}. \tag{2}$$

In general if $\Delta$ is an arbitrary $\Gamma$-invariant subset of $A^*$ and $\Delta^c$ its complement in $A^*$, the subspace of $KA$ defined by ( 2) is $A$-invariant.

**Theorem 12** *For $\tau \in A^*$, $\tau \in W_E$ if and only if $e_\tau \in W$.*

**Proof** Suppose $\tau \in A^*$. If $\tau \in W_E$, since $W_E$ is $\Gamma$-invariant

$$\Gamma\tau \subset W_E$$

and by theorem 7 $e_\tau \in W_E \cap KA = W$. Conversely, if $e_\tau \in W$, then by corollary 1 and the $A$-invariance of $W_E$

$$\tau e_\tau = \frac{1}{N}\tau \in W_E$$

proving the theorem.

Theorem 12 is the main result we need for describing $A$-invariant subspaces of $KA$ in terms of idempotents of $KA$.

**Corollary 11**

$$W = KAe_\Delta = \sum_{\tau \in \Delta/\Gamma} \oplus KAe_\tau,$$

*where* $\Delta = W_E \cap A^*$.

**Proof** By theorem 12, $e_\tau \in W$, for all $\tau \in \Delta$, implying $e_\Delta \in W$. Since $W$ is $A$-invariant, $KAe_\Delta \subset W$. Corollary 9 implies $1 = e_\Delta + e_{\Delta^c}$. By ( 2), for any $f \in W$,

$$f = f \cdot 1 = fe_\Delta + fe_{\Delta^c} = fe_\Delta,$$

completing the proof.

By corollary 11, every $A$-invariant subspace $W$ of $KA$ is generated by an idempotent $e_\Delta$, where $\Delta$ is the $\Gamma$-invariant subset $W_E \cap A^*$. By corollary 10, we have the following result.

**Corollary 12** *An $A$-invariant subspace $W$ of $KA$ is irreducible if and only if $W = KAe_\tau$, for some $\tau \in A^*$.*

The preceding discussion reduces the study of $A$-invariant subspaces of $KA$ to the study of $\Gamma$-invariant subsets on $A^*$. The irreducible $A$-invariant subspaces of $KA$ correspond to $\Gamma$-invariant subsets consisting of a single $\Gamma$-orbit. $A$-invariant subspaces of $KA$ which are the direct sums of, say $k$, irreducible $A$-invariant subspaces correspond to $\Gamma$-invariant subsets consisting of exactly $k$ distinct $\Gamma$-orbits. The following theorem summarizes these remarks.

**Theorem 13** *$KA$ is the direct sum of irreducible $A$-invariant subspaces*

$$KA = \sum_{\tau \in A^*/\Gamma} \oplus KA\tau.$$

*The number of irreducible $A$-invariant subspaces in $KA$ is equal to the number of $\Gamma$-orbits in $A^*$.*

*Every $A$-invariant subspace $W$ of $KA$ is the direct sum of irreducible $A$-invariant subspaces*

$$W = \sum_{\tau \in \Delta/\Gamma} \oplus KA\tau,$$

*where the number of irreducible $A$-invariant subspaces in $W$ is equal to the number of $\Gamma$-orbits in $W_E$.*

Suppose $G$ is an arbitrary finite group of order $N$ and $K$ is a field. Usually in examples and applications, $K = \mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ or a finite field $GF(p^R)$, $p$ a prime not dividing $N$, but results hold generally for fields whose characteristic does not divide $N$.

The *group algebra* $KG$ of $G$ over $K$ is the $K$-vector space of all formal sums

$$f = \sum_{t \in G} f(t)t, \qquad f(t) \in K,$$

under

$$f + g = \sum_{t \in G} (f(t) + g(t))\, t, \qquad f,\ g \in KG,$$

$$\alpha f = \sum_{t \in G} (\alpha f(t))\, t, \qquad f \in KG,\ \alpha \in K,$$

with $K$-algebra multiplication

$$fg = \sum_{t \in G} \left( \sum_{u \in G} f(u) g(u^{-1}t) \right) t, \qquad f,\ g \in KG.$$

The additions and multiplications inside the brackets are taken in $K$.

Generally since $G$ is not necessarily abelian, $fg$ is not necessarily equal to $gf$, $f,\ g \in KG$. Replacing $u$ by $tu^{-1}$ in the inner summation,

$$fg = \sum_{t \in G} \left( \sum_{u \in G} g(u) f(tu^{-1}) \right) t, \qquad f,\ g \in KG.$$

Denote by $L(G;K)$ the $K$-vector space of all $K$-valued functions on $G$. Every $f \in L(G;K)$ defines a formal sum in $KG$

$$f = \sum_{t \in G} f(t)t$$

and we can identify the $K$-vector space $KG$ with the $K$-vector space $L(G;K)$. The multiplication $fg$ in $KG$ corresponds to the possibly noncommutative convolution in $L(G;K)$

$$f * g(t) = \sum_{u \in G} f(u) g(u^{-1}t) = \sum_{u \in G} g(u) f(tu^{-1}), \qquad f,\ g \in L(G;K).$$

Under this identification the delta function $\delta_u$, $u \in G$, corresponds to a formal sum having a single nonzero coefficient which we denote by $u$,

$$u = \sum_{t \in G} \delta_u(t)t.$$

In this way we can view $G$ as a subset of $KG$ and a basis of the $K$-vector space $KG$.

For $u \in G$ and $f \in KG$,

$$uf = \sum_{t \in G} f(t)ut = \sum_{t \in G} f(u^{-1}t)t.$$

We call $uf$ the *left translation* of $f$ by $u$. Right translation can also be defined and generally differs from left translation, unless $G$ is abelian. For $u \in G$, the operator $L(u)$ of $KG$ defined by

$$L(u)f = uf, \quad f \in KG,$$

is a linear isomorphism of the $K$-vector space $KG$ and we have

$$L(uv) = L(u)L(v), \quad u, v \in G,$$

$$L(u^{-1}) = L(u)^{-1}, \quad u \in G,$$

where $L(u)L(v)$ and $L(u)^{-1}$ denote composition and inversion of operators on $KG$.

Denote by $GL(KG, K)$ the group of linear isomorphisms of the $K$-vector space $KG$. The mapping

$$L : G \to GL(KG, K)$$

is an isomorphism of the group $G$ into the group $GL(KG, K)$ called the *left-regular representation.*

A subspace $V$ of the $K$-vector space $KG$ is called $G$-*invariant* if for all $u \in G$,

$$uV = \{uf : f \in V\} \subset V.$$

A $G$-invariant subspace $V$ of $KG$ is called *irreducible* if the only $G$-invariant subspaces of $V$ are (0) and $V$. One of the main goals of nonabelian group harmonic analysis is to characterize the $G$-invariant, irreducible $G$-invariant and direct sum decompositions of $KG$ into irreducible $G$-invariant subspaces. For an abelian group, its character theory provided all the necessary tools for answering these questions. Generally these problems require a vast mathematical machinery for their solution. However for the nonabelian groups considered in this text, explicit solutions for many of these questions will be derived in terms of abelian group character theory.

For $g \in KG$, the operator $L(g)$ of $KG$ defined by

$$L(g)f = gf, \quad f \in KG,$$

is a linear homomorphism of the $K$-vector space $KG$. Since

$$L(g) = \sum_{t \in G} g(t)L(t), \quad g \in KG,$$

$G$-invariant subspace $V$ of $KG$ are $KG$-invariant subspaces. If $V$ is a $G$-invariant subspace of $KG$ and $f \in V$, then for all $g \in KG$,

$$gV \subset V.$$

Idempotent theory provides a convenient language in which to express many of the results in the following chapters. However explicit results can usually be written in terms of abelian group character concepts.

A nonzero element $e \in KG$ is called an *idempotent* if $e^2 = e$. Two idempotents $e_1$ and $e_2$ in $KG$ are called *orthogonal* if $e_1 e_2 = e_2 e_1 = 0$. A set of pairwise orthogonal idempotents

$$\{e_j : 1 \leq j \leq J\}$$

is said to be *complete* if

$$1 = \sum_{j=1}^{J} e_j.$$

**Example 23** If $e$ is an idempotent in $KG$, then $\{e, 1-e\}$ is a complete set of orthogonal idempotents.

**Example 24** If $e$ is an idempotent, then the $G$-invariant subspace generated by $e$, $KGe$, has $e$ as a right unit

$$KGe = \{\alpha \in KG : \alpha e = \alpha\}.$$

Simply write $\alpha \in KGe$ as $\alpha = \alpha' e$, $\alpha' \in KG$ and use

$$\alpha e = \alpha' e^2 = \alpha' e = \alpha.$$

Conversely if $\alpha \in KG$ can be written as $\alpha = \alpha e$, then $\alpha e \in KGe$ implies $\alpha \in KGe$.

**Example 25** If $e$ is an idempotent then $KG = KGe \oplus KG(1-e)$. Since $1 = e + (1-e)$, for any $\alpha \in KG$

$$\alpha = \alpha \cdot 1 = \alpha e + \alpha(1-e) \in KGe + KG(1-e)$$

and $KG = KGe + KG(1-e)$. The sum is a direct sum since if $\alpha \in KGe \cap KG(1-e)$ and we write $\alpha = \alpha' e = \alpha''(1-e)$, then

$$\alpha = \alpha' e = \alpha''(1-e)e = \alpha''(e - e^2) = 0.$$

The result described in example 25 holds generally for any complete set of orthogonal idempotents.

**Theorem 14** *If*

$$\{e_j : 1 \leq j \leq J\}$$

*is a complete set of orthogonal idempotents, then*

$$KG = \sum_{j=1}^{J} \oplus KGe_j.$$

**Proof** Since $1 = \sum_{j=1}^{J} e_j$, for any $\alpha \in KG$,

$$\alpha = \sum_{j=1}^{J} \alpha e_j \in \sum_{j=1}^{J} KGe_j$$

and $KG = \sum_{j=1}^{J} KGe_j$. If

$$0 = \sum_{j=1}^{J} \alpha_j e_j,$$

then for any $1 \leq k \leq J$, by orthogonality

$$0 = 0 \cdot e_k = \sum_{j=1}^{J} \alpha_j (e_j e_k) = \alpha_k e_k$$

proving the sum is a direct sum. The same argument shows the following corollary.

**Corollary 13** *If an idempotent $e$ can be written as the sum of two orthogonal idempotents, $e = e_1 + e_2$, then*

$$KGe = KGe_1 \oplus KGe_2.$$

**Example 26** If $KG = W_1 \oplus W_2$, where $W_1$ and $W_2$ are $G$-invariant subspaces and

$$1 = e_1 + e_2, \quad e_1 \in W_1,\ e_2 \in W_2,$$

then $\{e_1, e_2\}$ is a complete set of orthogonal idempotents. Since

$$e_1 = e_1 \cdot 1 = e_1^2 + e_1 e_2$$

with $e_1$, $e_1^2 \in W_1$ and $e_1 e_2 \in W_2$, by uniqueness of representation $e_1 = e_1^2$ and $e_1 e_2 = 0$. Now

$$e_1 = 1 \cdot e_1 = e_1^2 + e_2 e_1 = e_1 + e_2 e_1$$

implies $e_2 e_1 = 0$ verifying the example.

Generally we have the following result.

**Theorem 15** *If $KG$ is the direct sum of $G$-invariant subspaces*

$$KG = \sum_{j=1}^{J} \oplus W_j$$

*and*

$$1 = \sum_{j=1}^{J} e_j, \quad e_j \in W_j,\ 1 \leq j \leq J,$$

*then*

$$\{e_j : 1 \leq j \leq J\}$$

*is a complete set of orthogonal idempotents.*

**Proof** Completeness is by definition. For any $1 \leq k \leq J$,

$$e_k = e_k \cdot 1 = \sum_{j=1}^{J} e_k e_j$$

where $e_k e_j \in W_j$, $1 \leq j \leq J$, which by uniqueness of representation implies

$$e_k = e_k^2,\ e_k e_j = 0,\ j \neq k$$

competing the proof.

**Example 27** If $KGe = W_1 \oplus W_2$, the direct sum of $G$-invariant subspaces $W_1$ and $W_2$ with $e$ an idempotent and $e = e_1 + e_2$, $e_1 \in W_1$, $e_2 \in W_2$, then $e_1$ and $e_2$ are orthogonal idempotents. By example 24

$$e_1 = e_1 e = e_1^2 + e_1 e_2$$

which by uniqueness of representation implies

$$e_1 = e_1^2, \quad e_1 e_2 = 0.$$

The same argument shows that

$$e_2^2 = e_2, \quad e_2 e_1 = 0.$$

Generally we have the following which we state without proof.

**Theorem 16** *If $KGe$ is the direct sum of $G$-invariant subspaces*

$$KGe = \sum_{j=1}^{J} \oplus W_j,$$

*with $e$ an idempotent and*

$$e = \sum_{j=1}^{J} e_j, \quad e_j \in W_j,\ 1 \le j \le J,$$

*then*

$$\{e_j : 1 \le j \le J\}$$

*is a set of pairwise orthogonal idempotents.*

A homomorphism $P$ of the $K$-vector space $KG$ is called a *projection* if $P^2 = P$. If

$$\operatorname{im} P = \{P(\alpha) : \alpha \in KG\}$$

$$\ker P = \{\alpha \in KG : P(\alpha) = 0\},$$

then $\operatorname{im} P$ and $\ker P$ are subspaces of $KG$ satisfying

$$\operatorname{im} P = \{\alpha \in KG : P\alpha = \alpha\}$$

$$KG = \operatorname{im} P \oplus \ker P.$$

Every ~~sub~~space $W$ of $KG$ determines a projection $P$ such that $W = \operatorname{im} P$. Such a projection exists since if $KG = W \oplus W'$, for some subspace $W'$ of $KG$, then we can define $P$ by

$$P(w + w') = w, \quad w \in W,\ w' \in W'.$$

We will now show that every $G$-invariant subspace $W$ of $KG$ is generated by an idempotent. Consider any projection $P$ of $KG$ satisfying $W = \operatorname{im} P$ and define the mapping $P_0 : KG \to KG$ by

$$P_0(\alpha) = \frac{1}{N} \sum_{u \in G} u^{-1} P(u\alpha), \quad \alpha \in KG.$$

$P_0$ is a homomorphism of the $K$-vector space $KG$. Since $P(u\alpha) \in W$, $u \in G$ and $\alpha \in KG$, and $W$ is $G$-invariant

$$P_0(\alpha) \in W, \quad \alpha \in KG.$$

**Theorem 17** *For all* $\alpha \in KG$

$$P_0(\alpha) = \alpha P_0(1),$$

*and if* $\alpha \in W$, *then*

$$P_0(\alpha) = \alpha.$$

**Proof** For $t \in G$,

$$t^{-1}P_0(t) = \frac{1}{N}\sum_{u\in G} t^{-1}u^{-1}P(ut) = \frac{1}{N}\sum_{u\in G} u^{-1}P(u) = P_0(1),$$

by a change of variables. The linearity of $P_0$ proves the first part. If $\alpha \in W$, then $u\alpha \in W$, $u \in G$ and $P(u\alpha) = u\alpha$ implying

$$P_0(u\alpha) = \frac{1}{N}\sum_{u\in G} u^{-1}u\alpha = \alpha,$$

completing the proof.

Since $\operatorname{im} P_0 \subset W$ and $P_0$ acts by the identity mapping on $W$, by theorem 17 we have the following.

**Corollary 14** $P_0$ *is a projection of* $KG$ *satisfying* $W = \operatorname{im} P_0$.

Set $\overline{e} = P_0(1)$.

**Corollary 15** $e$ *is a generating idempotent for* $W$,

$$W = KGe, \qquad e^2 = e.$$

**Proof** By theorem 17 and corollary 14, for all $w \in W$,

$$w = P_0(w) = we.$$

Since $e \in W$, $e$ is an idempotent in $W$ and a right unit for $W$. Example 24 implies $W = KGe$, completing the proof.

Since every $G$-invariant subspace $W$ has a generating idempotent, by corollary 15, there exists a $G$-invariant subspace $W'$ such that $KG = W \oplus W'$. More generally we have the following result.

**Corollary 16** *If $W_1$ and $W_2$ are $G$-invariant subspaces of $KG$ such that $W_1 \subset W_2$ then there exists a $G$-invariant subspace $W_1'$ of $W_2$ such that $W_2 = W_1 \oplus W_1'$.*

**Proof** If $W'$ is a $G$-invariant subspace of $KG$ such that $KG = W_1 \oplus W'$, then $W_2 = W_1 \oplus (W' \cap W_2)$ where $W_1' = W' \cap W_2$ is a $G$-invariant subspace of $W_2$.

An idempotent $e \in KG$ is called *primitive* if $e$ can not be written as the sum of orthogonal idempotents in $KG$.

**Theorem 18** *$e$ is a primitive idempotent in $KG$ if and only if $KGe$ is irreducible.*

**Proof** If $e$ is not primitive and $e = e_1 + e_2$, where $e_1$ and $e_2$ are orthogonal idempotents, then $KG = KGe_1 \oplus KGe_2$ and $KGe$ is not irreducible. Conversely if $W$ is a $G$-invariant subspace of $KGe$, then by corollary 16, $KG = W \oplus W'$, for some $G$-invariant subspace $W'$ of $KGe$. Example 27 implies $e$ is not a primitive idempotent, completing the proof

The problem of constructing $G$-invariant, irreducible $G$-invariant and direct sum decompositions of $KG$ into irreducible $G$-invariant subspaces can be replaced by that of constructing idempotents, primitive idempotents and complete sets of primitive orthogonal idempotents.

Decompositions of $KG$ into direct sums of $G$-invariant subspaces

$$KG = \sum_{j=1}^{J} \oplus W_j$$

lead to block diagonal matrix representations of the left translation operators $L(\alpha)$, $\alpha \in KG$, and to fast algorithms for computing products in $KG$. Details for special groups $G$ will be given in the following chapters. However, in this chapter we will describe the general outline of the method.

For $t \in G$, the matrix $S(t)$ of $L(t)$ relative to the basis $G$, of $KG$, ordered in some way, is a permutation matrix reflecting the group structure of $G$. The matrix $S(\alpha)$ of $L(\alpha)$, $\alpha \in KG$, relative to $G$ is a linear combination over $K$ of the permutation matrices $S(t)$, $t \in G$. If $G$ is a cyclic group, then the corresponding matrices $S(t)$, $t \in G$, are cyclic shift matrices and the corresponding matrices $S(\alpha)$, $\alpha \in KG$, are circulant matrices. In this case the direct sum decomposition of $KG$ given by the characters diagonalizes the circulant matrices with the Fourier transform describing the change of basis.

Generally since $W_j$ is $G$-invariant, $L(\alpha)$, $\alpha \in KG$, maps $W_j$ into itself. Denoting by $T_j(\alpha)$ the matrix of the restriction of $L(\alpha)$ to some basis of $W_j$, the matrix direct sum

$$T(\alpha) = \sum_{j=1}^{J} T_j(\alpha),$$

is the matrix representation of $L(\alpha)$ relative to the basis of $KG$ formed by piecing together the bases from the $W_j$, $1 \leq j \leq J$. We say the new basis is compatible with the direct sum decomposition of $KG$.

To compute

$$\alpha\beta = L(\alpha)\beta, \qquad \alpha, \beta \in KG,$$

we write $\beta$ in terms of the compatible basis, compute $T(\alpha)$ and form the matrix product of $T(\alpha)$ with the coordinates of $\beta$ in the compatible basis and then translate the result back to the basis $G$.

# 6 Group algebras of $A \leftthreetimes B$

A subgroup $A$ of a group $G$ is called *normal* if for all $t \in G$,

$$tAt^{-1} = \{tat^{-1} : a \in A\} \subset A.$$

$G$ is said to be the *semidirect product* of a normal group $A$ and a subgroup $B$ if every $t \in G$ can be written uniquely as

$$t = xy, \quad x \in A,\ y \in B.$$

In this case we write $G = A \leftthreetimes B$ and we call $x$ the *A-component* and $y$ the *B-component* of $t$. If $t = xy$ and $t' = x'y'$ with $x, x' \in A$, $y, y' \in B$ then

$$tt' = x(yx'y^{-1})yy'$$

where $x(yx'y^{-1})$ is the $A$-component and $yy'$ is the $B$ component of $tt'$.

In this chapter we will study groups of the form $G = A \leftthreetimes B$ where $A$ and $B$ are abelian groups.

For $\alpha \in KA$ and $\beta \in KB$, we can view $\alpha, \beta \in KG$. If $\alpha\beta = 0$, then

$$\sum_{x \in A} \sum_{y \in B} \alpha(x)\beta(y)xy = 0$$

which implies

$$\alpha(x)\beta(y) = 0, \quad x \in A,\ y \in B,$$

and $\alpha = 0$ or $\beta = 0$.

## 6.1 Split case

Suppose $G = A \leftthreetimes B$ where $A$ and $B$ are abelian groups splitting over $K$. Denote the character groups of $A$ and $B$ over $K$ by $A^*$ and $B^*$. If $\tau \in A^*$ and $\lambda \in B^*$, then as elements in $KG$

$$\tau = \sum_{x \in A} \tau(x)x, \quad \tau(x) \in K,$$

and

$$\lambda = \sum_{y \in B} \lambda(y)y, \quad \lambda(y) \in K.$$

$B$ acts on $A^*$. For $\tau \in A^*$ and $y \in B$ define $\tau^y \in KG$ by

$$\tau^y = y\tau y^{-1}.$$

Since $A$ is a normal subgroup of $G$

$$\tau^y = \sum_{x \in A} \tau(x)yxy^{-1} = \sum_{x \in A} \tau(y^{-1}xy)x$$

is also in $A^*$. For $y, y' \in B$

$$(\tau^y)^{y'} = \tau^{y'y}$$

and as a special case

$$(\tau^y)^{y^{-1}} = \tau.$$

For $\tau \in A^*$

$$B\tau = \{\tau^y : y \in B\}$$

is a subset of $A^*$ called the $B$-orbit over $\tau$.

If $\tau$ and $\tau'$ are in $A^*$ and $\tau' \in B\tau$ with $\tau' = \tau^y$, $y \in B$, then

$$\tau = (\tau^y)^{y^{-1}} = \tau'^{y^{-1}} \in B\tau'$$

and $B\tau = B\tau'$.

For $\tau$ and $\tau'$ in $A^*$, if $B\tau \cap B\tau' \neq \phi$, with $\tau^y = \tau'^{y'}$, $y, y' \in B$, then

$$\tau = (\tau^y)^{y^{-1}} = \left((\tau')^{y'}\right)^{y^{-1}} = \tau'^{y^{-1}y'}$$

and $\tau \in B\tau'$ implying $B\tau = B\tau'$. Consequently $A^*$ is partitioned into the disjoint union of distinct $B$-orbits. A set

$$\{\tau_1, \ldots, \tau_K\} \subset A^*$$

is called a *complete set of representatives* for the collection $A^*/B$ of distinct $B$-orbits in $A^*$ if $A^*$ is the disjoint union

$$A^* = \sum_{k=1}^{K} B\tau_k.$$

Since

$$1 = \frac{1}{L}\sum_{\tau \in A^*} \tau, \qquad 1 = \frac{1}{M}\sum_{\lambda \in B^*} \lambda,$$

where $L$ and $M$ are the orders of $A$ and $B$

$$1 = \frac{1}{N}\sum_{\tau \in A^*}\sum_{\lambda \in B^*} \tau\lambda,$$

where $N = LM$ is the order of $G$. However generally $\tau$ and $\lambda$ do not commute. We do have the following.

**Theorem 19** *For $t = xy \in G$, $x \in A$, $y \in B$,*

$$t = \frac{1}{N}\sum_{\tau \in A^*}\sum_{\lambda \in B^*} \tau^y(x^{-1})\lambda(y^{-1})\tau^y\lambda.$$

**Proof** Since $x\tau^y = \tau^y(x^{-1})\tau^y$ and $y\lambda = \lambda(y^{-1})\lambda$,

$$t\tau\lambda = xy\tau\lambda = x\tau^y y\lambda = \tau^y(x^{-1})\lambda(y^{-1})\tau^y\lambda$$

completing the proof.

Since $G$ is a basis of the $K$-vector space $KG$, by theorem 19, the collection of products in $KG$

$$\{\tau\lambda : \tau \in A^*,\ \lambda \in B^*\}$$

is also a basis of $KG$. Generally $KG\tau\lambda$ is not one-dimensional, so that the spaces

$$\{KG\tau\lambda : \tau \in A^*,\ \lambda \in B^*\}$$

intersect. If $G$ is abelian, then the products $\tau\lambda$, $\tau \in A^*$, $\lambda \in B^*$, are the characters of $G$ over $K$ and the results of chapter 4 apply.

Generally to form direct sum decompositions of $KG$ into left $G$-invariant subspaces we must modify the above approach. For $\tau \in A^*$, define

$$B(\tau) = \{y \in B : \tau^y = \tau\}.$$

$B(\tau)$ is a subgroup of $B$ called the *centralizer* of $\tau$ in $B$.

Suppose $\tau_1$, $\tau_2 \in A^*$ with $\tau_2 = \tau_1^{y_1}$, $y_1 \in B$. If $y \in B(\tau_1)$, then since $B$ is abelian

$$\tau_2^y = (\tau_1^{y_1})^y = (\tau^y)^{y_1} = \tau^{y_1} = \tau_2$$

and $y \in B(\tau_2)$ proving the following result.

**Theorem 20** *If* $\tau_2 \in B\tau_1$, $\tau_1$, $\tau_2 \in A^*$, *then*

$$B(\tau_1) = B(\tau_2).$$

We can assign a centralizer in $B$ to every $B$-orbit in $A^*$. The assumption that $B$ is abelian is essential.

Suppose $\tau \in A^*$ and consider $B(\tau)$. For $y \in B$, the set

$$yB(\tau) = \{yz : z \in B(\tau)\} \subset B$$

is called the left *coset* of $B(\tau)$ in $B$ determined by $y$. If $y' \in B(\tau)$, then $y'B(\tau) = yB(\tau)$. The usually arguments show that two left cosets are either equal or else have empty intersection. The collection $B/B(\tau)$ of left cosets of $B(\tau)$ in $B$ forms a partition of $B$. A set

$$\{y_s : 1 \le s \le S\} \subset B$$

is called a *complete system of representatives* of $B/B(\tau)$ if $B$ is the disjoint union

$$B = \sum_{s=1}^{S} y_s B(\tau).$$

Since $B$ is an abelian group, a group structure can be placed on $B/B(\tau)$ by

$$yB(\tau)y'B(\tau) = yy'B(\tau)$$

$$(yB(\tau))^{-1}y^{-1}B(\tau), \quad y,\ y' \in B.$$

For $y \in y_sB(\tau)$, with $y = y_sz$, $1 \leq s \leq S$, $z \in B(\tau)$,

$$\tau^y = (\tau^z)^{y_s} = \tau^{y_s}, \quad 1 \leq s \leq S.$$

Moreover if $\tau^{y_s} = \tau^{y_t}$, $1 \leq s,\ t \leq S$, then

$$\tau^{y_t^{-1}y_s} = \tau$$

and $y_sB(\tau) = y_tB(\tau)$. Consequently the $B$-orbit $B\tau$ has order $S$ and

$$B\tau = \{\tau^{y_s} : 1 \leq s \leq S\}.$$

Generally the $y_s$, $1 \leq s \leq S$ depend on $\tau$ and when we need to express the dependence we write $y_s^\tau$, $1 \leq s \leq S_\tau$. If $M_\tau$ denotes the order of $B(\tau)$,then $M = M_\tau S_\tau$, where $M$ is the order of $B$.

We will now show that the collection of products

$$\frac{1}{L}\frac{1}{M_\tau}\tau\lambda, \qquad \tau \in A^*,\ \lambda \in B(\tau)^*,$$

forms a complete set of primitive orthogonal idempotents for $KG$. We break up the proof into the following three theorems.

**Theorem 21** *For $\tau_1,\ \tau_2 \in A^*$ and $\lambda_1 \in B(\tau_1)^*$, $\lambda_2 \in B(\tau_2)^*$,*

$$(\tau_1\lambda_1)^2 = LM_{\tau_1}\tau_1\lambda_1$$

*and*

$$(\tau_1\lambda_1)(\tau_2\lambda_2) = 0, \text{ unless } \tau_1 = \tau_2 \text{ and } \lambda_1 = \lambda_2.$$

**Proof** Since $\tau_1^y = \tau_1$, $y \in B(\tau_1)$,

$$\tau_1\lambda_1 = \sum_{y \in B(\tau_1)} \lambda_1(y)\tau_1 y = \sum_{y \in B(\tau_1)} \lambda_1(y) y\tau_1 = \lambda_1\tau_1.$$

Consequently

$$(\tau_1\lambda_1)^2 = \lambda_1\tau_1^2\lambda_1 = L\tau_1\lambda_1^2 = LM_{\tau_1}\tau_1\lambda_1$$

and

$$(\tau_1\lambda_1)(\tau_2\lambda_2) = \lambda_1(\tau_1\tau_2)\lambda_2 = 0, \text{ unless } \tau_1 = \tau_2,$$

in which case

$$(\tau_1\lambda_1)(\tau_1\lambda_2) = \tau_1\lambda_1\lambda_2 = 0, \text{ unless } \lambda_1 = \lambda_2,$$

completing the proof.

By theorem 21, the collection of products is a set of orthogonal idempotents in $KG$.

**Theorem 22**

$$1 = \sum_{\tau\in A^*} \sum_{\lambda\in B(\tau)^*} \frac{1}{L}\frac{1}{M_\tau}\tau\lambda.$$

**Proof** The theorem follows from

$$1 = \frac{1}{L}\sum_{\tau\in A^*} \tau$$

and

$$1 = \frac{1}{M_\tau}\sum_{\lambda\in B(\tau)^*} \lambda, \quad \tau \in A^*.$$

Theorem 22 implies completeness.

For $\tau \in A^*$ and $\lambda \in B(\tau)^*$, by theorem 21

$$e = \frac{1}{LM_\tau}\tau\lambda$$

is an idempotent. Since $\frac{1}{L}\tau$ is an idempotent and $\tau\lambda = \lambda\tau$

$$e = \frac{1}{L}\tau e = \frac{1}{L}e\tau.$$

**Theorem 23** *If $\tau \in A^*$ and $\lambda \in B(\tau)^*$, then $e = \frac{1}{LM_\tau}\tau\lambda$ is a primitive idempotent.*

**Proof** Assume $e$ is not primitive and $e = e_1 + e_2$ where $e_1$ and $e_2$ are orthogonal idempotents. Since

$$e_1 = e_1 e = \frac{1}{L}e_1 e\tau = \frac{1}{L}e_1\tau$$

and

$$e_1 = ee_1 = \frac{1}{L}\tau e e_1 = \frac{1}{L}\tau e_1$$

we have

$$e_1 = e_1^2 = \frac{1}{L^2}\tau e_1^2\tau = \frac{1}{L^2}\tau e_1\tau.$$

Since $A^*$ is a basis of $KA$, we can write

$$e_1 = \frac{1}{L}\sum_{y\in B}\left(\sum_{\tau'\in A^*} e_1(\tau',y)\tau'\right)y, \qquad e_1(\tau',y)\in K.$$

Consequently

$$e_1 = \frac{1}{L^2}\tau e_1\tau = \frac{1}{L^3}\sum_{y\in B}\sum_{\tau'\in A^*} e_1(\tau',y)\tau\tau' y\tau.$$

However

$$\tau\tau' y\tau = 0, \text{ unless } \tau' = \tau \text{ and } y\in B(\tau),$$

and

$$\tau^2 y\tau = L^2\tau y, \qquad y\in B(\tau),$$

implying

$$e_1 = \frac{1}{L}\tau\sum_{y\in B(\tau)} e_1(\tau,y)y = \frac{1}{L}\tau m_1, \qquad m_1\in KB(\tau).$$

The same argument shows that

$$e_2 = \frac{1}{L}\tau m_2, \qquad m_2\in KB(\tau),$$

implying

$$e = \frac{1}{LM_\tau}\tau\lambda = \frac{1}{L}\tau(m_1+m_2).$$

Since $\overline{\tau}\in KA$ and $\lambda,\ m_1+m_2\in KB(\tau)$,

$$\frac{1}{M_\tau}\lambda = m_1+m_2.$$

We will show that $m_1$ and $m_2$ are orthogonal idempotents in $KB(\tau)$, contradicting the fact that $\frac{1}{M_\tau}\lambda$ is a primitive idempotent in $KB(\tau)$.

Since $\tau m_1 = m_1\tau$,

$$e_1^2 = \frac{1}{L}\tau m_1^2 = \frac{1}{L}\tau m_1$$

implying $m_1^2 = m_1$. The same argument shows $m_2^2 = m_2$ and $m_1m_2 = m_2m_1 = 0$, completing the proof.

We have proved that the collection of products

$$\frac{1}{LM_\tau}\tau\lambda : \tau\in A^*,\ \lambda\in B(\tau)^*$$

is a complete set of primitive orthogonal idempotents for $KG$ and we can apply the results of the previous chapter.

**Theorem 24**

$$KG = \sum_{\tau \in A^*} \sum_{\lambda \in B(\tau)^*} \oplus KG\tau\lambda$$

*with the direct sum factors*

$$KG\tau\lambda, \quad \tau \in A^*, \ \lambda \in B(\tau)^*,$$

*irreducible $G$-invariant subspaces of $KG$.*

In the abelian case, the irreducible $G$-invariant subspaces of $KG$ are one-dimensional and are uniquely determined by the characters. The Fourier transform is the change of basis transform between the $G$-basis and the character basis. The importance of the Fourier transform in digital signal processing is greatly enhanced by fast algorithms for the Fourier transform.

In contrast, if $G$ is not abelian, an irreducible $G$-invariant subspace of $KG$ is not necessarily one-dimensional. For groups of the form $G = A \leftthreetimes B$, with $A$ and $B$ abelian, we will determine bases for the subspaces $KG\tau\lambda$, $\tau \in A^*$, $\lambda \in B(\tau)^*$, and derive fast algorithms for relating components in the $G$-basis to components in the new basis.

Suppose $\tau \in A^*$ and $\lambda \in B(\tau)^*$. Set $y_s = y_s^\tau$, $1 \le s \le S = S_\tau$ in the following discussion. For $x \in A$ and $y \in B$, with $y = y_s z$, $1 \le s \le S$ and $z \in B(\tau)$,

$$\begin{aligned} xy\tau\lambda &= xy_s z\tau\lambda = x\tau^{y_s} y_s z\lambda \\ &= \tau^{y_s}(x^{-1})\lambda(z^{-1})y_s\tau\lambda. \end{aligned}$$

**Theorem 25** *For $\tau \in A^*$ and $\lambda \in B(\tau)^*$, the set*

$$\{y_s\tau\lambda : 1 \le s \le S\}$$

*is a basis of the $K$-vector space $KG\tau\lambda$.*

**Proof** Since the set

$$\{xy\tau\lambda : x \in A, \ y \in B\}$$

spans $KG\tau\lambda$, the set

$$\{y_s\tau\lambda : 1 \le s \le S\}$$

spans $KG\tau\lambda$. We must show that this set is linearly independent. Suppose that

$$0 = \sum_{s=1}^{S} \alpha(s) y_s\tau\lambda, \quad \alpha(s) \in K, \ 1 \le s \le S.$$

Multiplying on the left by $\tau^{y_t}$, $1 \le t \le S$,

$$\begin{aligned} 0 = \tau_t^y 0 &= \sum_{s=1}^{S} \alpha(s) \tau^{y_t} \tau^{y_s} y_s \lambda \\ &= L\alpha(t) y_t \tau \lambda \end{aligned}$$

implying $\alpha(t) = 0$. Since $t$ is arbitrary, $1 \le t \le S$, $\alpha(t) = 0$, for all $1 \le t \le S$, completing the proof.

For $\alpha \in KG$,

$$\alpha = \frac{1}{L} \sum_{\tau \in A^*} \frac{1}{M_\tau} \sum_{\lambda \in B(\tau)^*} \alpha \tau \lambda$$

and by theorem 25

$$\frac{1}{L} \frac{1}{M_\tau} \alpha \tau \lambda = \sum_{s=1}^{S_\tau} \alpha_{\tau\lambda}(s) y_s^\tau \tau \lambda, \qquad \alpha_{\tau\lambda}(s) \in K.$$

**Theorem 26** *For $\alpha \in KG$, $\tau \in A^*$ and $\lambda \in B(\tau)^*$,*

$$\alpha_{\tau\lambda}(s) = \frac{1}{L} \frac{1}{M_\tau} \sum_{z \in B(\tau)} \left( \sum_{x \in A} \alpha(x y_s z) \tau^{y_s}(x^{-1}) \right) \lambda(z^{-1}),$$

*where $y_s = y_s^\tau$, $1 \le s \le S$.*

**Proof** Since

$$\alpha \tau \lambda = \sum_{s=1}^{S_\tau} \sum_{z \in B(\tau)} \sum_{x \in A} \alpha(x y_s z) x y_s z \tau \lambda,$$

the theorem follows from

$$x y_s z \tau \lambda = \tau^{y_s}(x^{-1}) \lambda(z^{-1}) y_s \tau \lambda, \qquad z \in B(\tau),\ 1 \le s \le S_\tau.$$

We will now use theorem 26 to derive an algorithm for computing the coefficients

$$\alpha_{\tau\lambda}(s), \qquad \tau \in A^*,\ \lambda \in B(\tau)^*,\ 1 \le s \le S_\tau,$$

based on abelian group Fourier transforms.

For $y \in B$, define $\alpha_y \in KA$ by

$$\alpha_y(x) = \alpha(xy), \qquad x \in A,$$

and compute the Fourier transform of $\alpha_y$ over $A$,

$$\hat{\alpha_y}(\tau) = \frac{1}{L} \sum_{x \in A} \alpha_y(x) \tau(x^{-1}), \quad \tau \in A^*.$$

$M$ Fourier transforms over $A$ are required at this stage. Place the results into a two-dimensional array over $A^* \times B$

$$\hat{\alpha}(\tau, y) = \hat{\alpha_y}(\tau), \quad \tau \in A^*, \ y \in B.$$

For each $\tau \in A^*$ we will compute the coefficients

$$\alpha_{\tau\lambda}(s), \quad 1 \leq s \leq S_\tau, \ \lambda \in B(\tau)^*.$$

For $1 \leq s \leq S_\tau$, define $\gamma_s^\tau \in KB(\tau)$ by

$$\gamma_s^\tau(z) = \hat{\gamma}(\tau^{y_s}, y_s z), \quad z \in B(\tau), \ y_s = y_s^\tau,$$

and compute the Fourier transform of $\gamma_s^\tau$ over $B(\tau)$

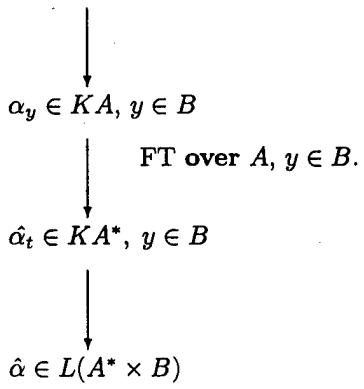
$$\hat{\gamma_s^\tau}(\lambda) = \frac{1}{M_\tau} \sum_{z \in B(\tau)} \gamma_s^\tau(z) \lambda(z^{-1}), \quad \lambda \in B(\tau)^*.$$

$S_\tau$ Fourier transforms over $B(\tau)$ are required in this stage. Implementing this stage as $\tau$ runs over $A^*$ requires $\sum_{\tau \in A^*} S_\tau$ Fourier transforms over abelian groups over varying sizes.

By theorem 26, for each $\tau \in A^*$,

$$\alpha_{\tau\lambda}(s) = \hat{\gamma_s^\tau}(\lambda), \quad \lambda \in B(\tau)^*, \ 1 \leq s \leq S_\tau.$$

**First Stage** $\alpha \in KG$



**Second Stage** $\tau \in A^*$

$$\hat{\alpha} \in L(A^* \times B)$$

$$\downarrow$$

$$\gamma_s^\tau \in KB(\tau),\ 1 \le s \le S_\tau$$

$$\downarrow \quad \text{FT over } B(\tau),\ 1 \le s \le S_\tau.$$

$$\hat{\gamma}_s^\tau \in KB(\tau)^*,\ 1 \le s \le S_\tau$$

$$\alpha_{\tau\lambda}(s) = \hat{\gamma}_s^\tau(\lambda), \quad \lambda B(\tau)^*,\ 1 \le s \le S_\tau.$$

The algorithm computes the coefficients

$$\alpha_{\tau\lambda}(s), \quad \tau \in A^*,\ \lambda \in B(\tau)^*,\ 1 \le s \le S_\tau$$

by first computing $M$ Fourier transforms over $A$ and then partitioning the remaining computation into $L$ parallel stages parameterized by $\tau \in A^*$. For each $\tau \in A^*$, we implement a data rearrangement step which forms $S_\tau$ elements in $KB(\tau)$ and then computes $S_\tau$ Fourier transforms over $B(\tau)$. For $\lambda \in B(\tau)^*$, the $S_\tau$-coefficients

$$\alpha_{\tau\lambda}(s), \quad 1 \le s \le S_\tau,$$

are given by evaluation of the $S_\tau$ Fourier transforms at $\lambda$.

Assuming that the Fourier transform over an abelian group of size $P$ requires $P \log P$ complex add-multiplies, the first stage requires $N \log L$ complex add-multiplies to implement $M$ Fourier transforms over $A$. For each $\tau \in A^*$, the second stage requires $M \log M_\tau$ complex add-multiplies, since $M = S_\tau M_\tau$, to implement $S_\tau$ Fourier transforms over $B(\tau)$. To implement the second stage over all $\tau \in A^*$ requires $M \sum_{\tau \in A^*} \log M_\tau$ complex add-multiplies. The complete algorithm requires

$$N \log L + M \sum_{\tau \in A^*} \log M_\tau$$

complex add-multiplies.

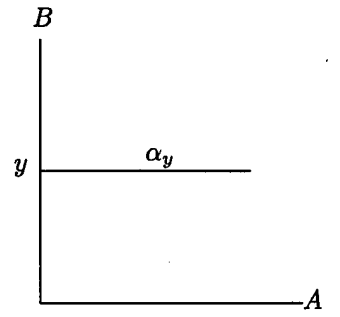
Up to scale multiple, the abelian Fourier transform can be realized by a unitary matrix which relates the coefficients over $G$ with the coefficients over the character basis. Since the relationship between the coefficients over $G$ with the coefficients over the basis

$$\{y_s^\tau \tau\lambda : \tau \in A^*,\ \lambda \in B(\tau)^*,\ 1 \leq s \leq S_\tau\}$$

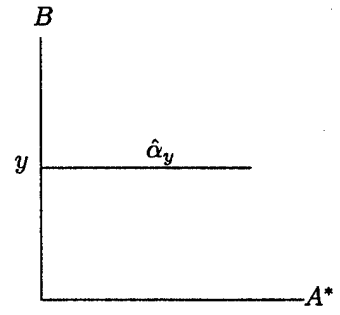
is based on abelian group Fourier transforms we can represent the mapping between these coefficients by a unitary matrix, up to scale multiple, as well.

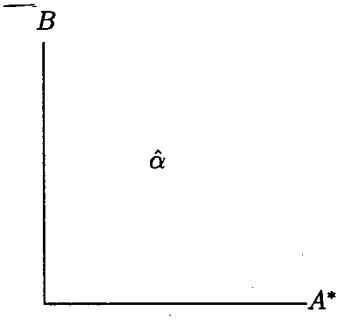
The algorithm can be displayed by the following four pictures.

**Fourier transform over $A$**




$\alpha_y(x) = \alpha(xy)$, $x \in A$, $y \in B$.

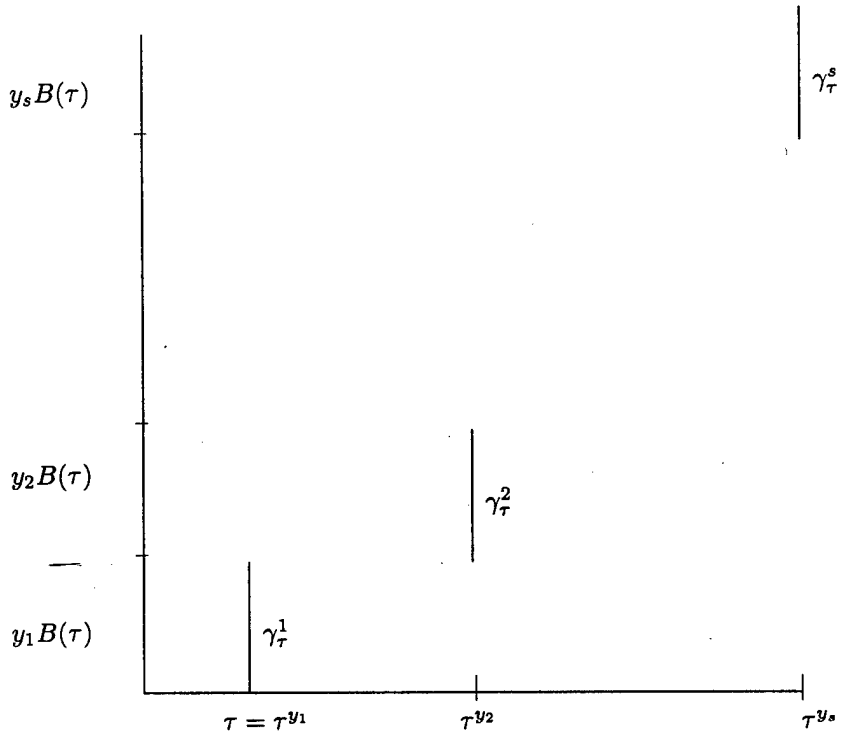


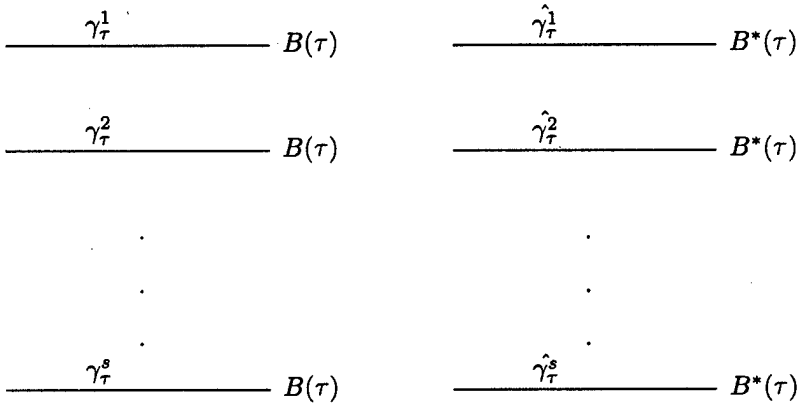

$\hat{\alpha}(\tau, y) = \hat{\alpha}_y(\tau)$, $\tau \in A^*$.

**Data readdressing**

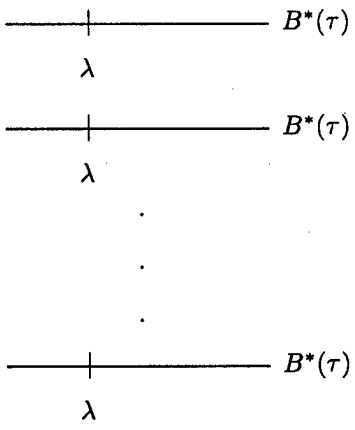
$$\alpha_\tau^s(z) = \hat{\alpha}(\tau^{y_s}, y_s z), \qquad z \in B(\tau),\ 1 \le s \le S_\tau.$$



**Fourier transform over $B(\tau)$.**




**Data readdressing**




$\alpha_{\tau\lambda}(s) = \hat{\gamma}_\tau^s(\lambda), 1 \leq s \leq S_\tau,\ \tau \in A^*,\ \lambda \in B(\tau)^*.$

From the first data rearrangement stage we can see how non-commutativity affects the classical abelian group two-dimensional Fourier transform $A \times B$. If $B(\tau) = B$, then $S_\tau = 1$ and the next stage Fourier transform is over all of $B$. For $B(\tau) = (0)$, $S = M$, the order of $B$, and the data passes through unchanged. No Fourier transform is required. If $B(\tau)$ is a proper subgroup of $B$, the Fourier transform of the decimated data over $B(\tau)$ produces a periodization of the Fourier transform over $B$. Generally the coefficients $\alpha_{\tau\lambda}(s)$ represent periodizations and phase modulated periodizations of the Fourier transform over $B$ of the Fourier transform of the initial data with respect to $A$.

# 7 Examples

## 7.1 The Dihedral Group $D_N = C_N \leftthreetimes C_2$

Denote the elements of $C_N$ by $a^n$, $0 \leq n \leq N-1$, and characters of $C_N$ by $\alpha_k$, $0 \leq k \leq N-1$,

$$\alpha_k = \sum_{n=0}^{N-1} exp(2\pi i \frac{kn}{N}) a^n.$$

Let $D_N = C_N \leftthreetimes C_2$, the dihedral group of order $2N$.

$$D_N = \langle a,\ t;\ a^N = t^2 = 1,\ tat = a^{-1} \rangle.$$

### 7.1.1 Group convolution

For $f, g \in \mathbf{C}D_N$,

$$f = \sum_{x \in D_N} f(x)x, \quad g = \sum_{x \in D_N} g(x)x, \qquad f(x), g(x) \in \mathbf{C},$$

the $\mathbf{C}$-algebra multiplication is defined by

$$fg = \sum_{y \in D_N} \left( \sum_{x \in D_N} f(x) g(x^{-1}y) \right) y.$$

### 7.1.2 Complete system of orthogonal idempotents

Complete system of orthogonal idempotents of $C_2$ are

$$(1+t)/2,\ (1-t)/2.$$

- $2 \nmid N$

$$C_2(\alpha_k) = \begin{cases} C_2, & k = 0 \\ \{1\}, & \text{otherwise.} \end{cases}$$

A complete set of primitive idempotents of $\mathbf{C}D_N$ are

$$\frac{1}{N}\{\alpha_0(1+t)/2,\ \alpha_0(1-t)/2,\ \alpha_n,\ 1 \leq n \leq N-1\}.$$

$\frac{1}{2N}\alpha_0(1+t)$ and $\frac{1}{2N}\alpha_0(1-t)$ are of dimension 1, while $\frac{1}{N}\alpha_n$, $1 \leq n \leq N-1$ are of dimension 2.

- $N = 2M$

$$C_2(\alpha_k) = \begin{cases} C_2, & k = 0, \text{ or } M \\ \{1\}, & \text{otherwise.} \end{cases}$$

Thus complete set of primitive idempotents of $\mathbf{C}D_{2M}$ are

$$\frac{1}{N}\{\alpha_0(1+t)/2,\ \alpha_0(1-t)/2,\ \alpha_M(1+t)/2,$$
$$\alpha_M(1-t)/2, \alpha_n,\ 1 \le n \le 2M-1,\ n \ne M\}.$$

$\frac{1}{2N}\alpha_0(1 \pm t)$ and $\frac{1}{2N}\alpha_M(1 \pm t)$ are of dimension 1, while $\frac{1}{N}\alpha_n$, $1 \le n \le N-1$, $n \ne M$, are of dimension 2.

### 7.1.3 Basis of orthogonal idempotents

- $2 \nmid N$

$$\frac{1}{N}\{\frac{1}{2}\alpha_0(1+t), \alpha_n, \frac{1}{2}\alpha_0(1-t), t\alpha_n,\ 1 \le n \le N-1\}$$

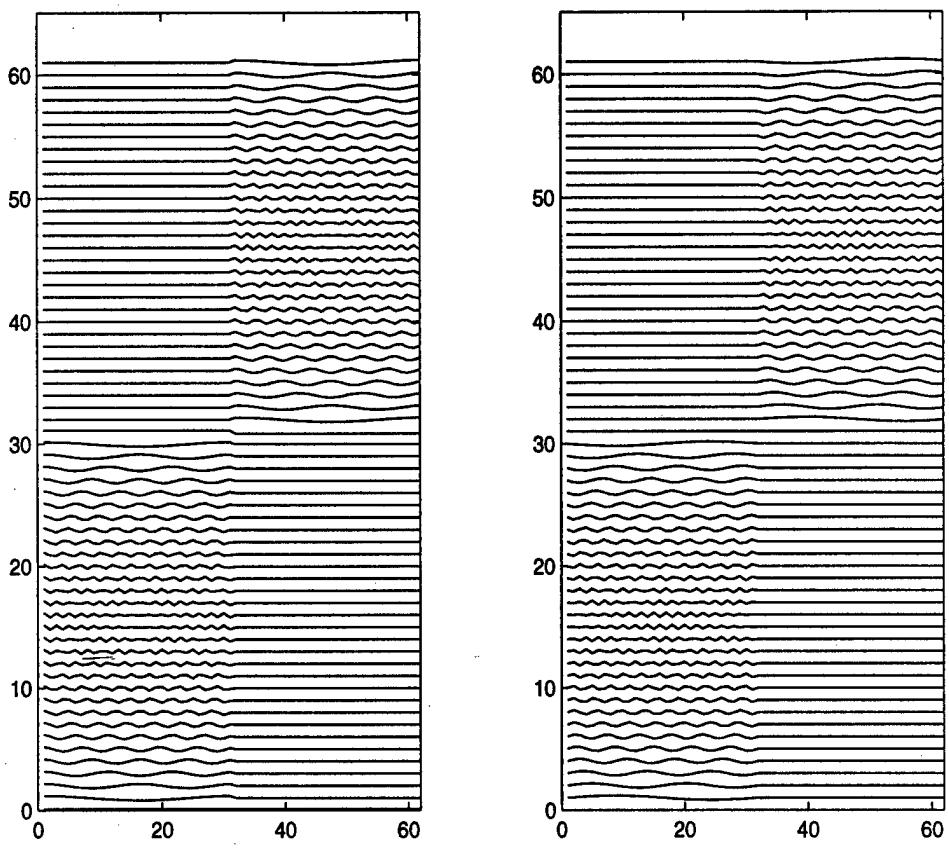
is a basis of $CD_N$. The one-dimensional orthogonal idempotent basis elements correspond to the one-dimensional invariant subspaces. The pairs of basis elements $\frac{1}{N}\{\alpha_n, t\alpha_n\}$, $1 \le n \le N-1$ corresponds to the two-dimensional invariant subspaces.

- $N = 2M$

$$\frac{1}{N}\{\frac{1}{2}\alpha_0(1+t), \alpha_m, \frac{1}{2}\alpha_0(1-t), t\alpha_m, \frac{1}{2}\alpha_M(1+t),$$
$$\alpha_{M+m}, \alpha_M(1-t), t\alpha_{M+m},\ 1 \le m \le M-1\}$$

is a basis of $CD_{2M}$. The one-dimensional orthogonal idempotent basis elements correspond to the one-dimensional invariant subspaces. The pairs of basis elements $\frac{1}{N}\{\alpha_m, t\alpha_m\}$, $\frac{1}{N}\{\alpha_{M+m}, t\alpha_{M+m}\}$, $1 \le m \le M-1$ corresponds to the two-dimensional invariant subspaces.

Figure 1: Profile of the basis vectors for $\mathbf{C}(C_{32} \wr C_2)$




The matrix of the new basis block-diagonalizes the group convolution, with the computational complexity of $2N \log N$. The diagonal blocks correspond to the invariant subspaces, and are of sizes 1 or 2. The group convolution can be computed by the following algorithm.

Denote the matrix of the new basis by $\Gamma(D_N)$. For $f, g \in \mathbf{C}D_N$, let $h = fg$.

1. Compute $\hat{f} = \Gamma(D_N)f$ and $\hat{g} = \Gamma(D_N)g$.

2. • For $2 \nmid N$, compute $\hat{h}$ by

$$\hat{h}(0) = \hat{f}(0)\hat{g}(0), \qquad \hat{h}(N) = \hat{f}(N)\hat{g}(N),$$

$$\hat{h}(k) = \hat{f}(k)\hat{g}(k) + \hat{f}(N+k)\hat{g}(2N-k),$$
$$\hat{h}(k+N) = \hat{f}(k)\hat{g}(N+k) + \hat{f}(N+k)\hat{g}(N-k),$$
$$1 \le k \le N-1.$$

- For $N = 2M$, compute $\hat{h}$ by

$$\hat{h}(0) = \hat{f}(0)\hat{g}(0), \quad \hat{h}(M) = \hat{f}(M)\hat{g}(M),$$
$$\hat{h}(N) = \hat{f}(N)\hat{g}(N), \quad \hat{h}(N+M) = \hat{f}(N+M)\hat{g}(N+M),$$
$$\hat{h}(k) = \hat{f}(k)\hat{g}(k) + \hat{f}(N+k)\hat{g}(2N-k),$$
$$\hat{h}(k+N) = \hat{f}(k)\hat{g}(N+k) + \hat{f}(N+k)\hat{g}(N-k),$$
$$1 \le k \le N-1,\ k \ne M.$$

3. Compute $h = \Gamma(D_N)^{-1}\hat{h}$.

## 7.2 The Dihedral Group $(C_N \times C_N) \leftthreetimes C_2$

Denote the elements of $C_N \times C_N$ by $a^m b^n$, $0 \le m, n \le N-1$, and characters of $C_N \times C_N$ by $\alpha_k\beta_l$, $0 \le k, l \le N-1$,

$$\alpha_k\beta_l = \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} exp(2\pi i\frac{km+ln}{N})a^m b^n.$$

$$(C_N \times C_N) \leftthreetimes C_2 = \langle a,\ b,\ t;\ a^N = b^N = t^2 = 1,\ ab = ba,\ tat = b,\ tbt = a\rangle.$$

### 7.2.1 Complete system of orthogonal idempotents

Complete system of orthogonal idempotents of $C_2$ are

$$(1+t)/2,\ (1-t)/2.$$

$$C_2(\alpha_k\beta_l) = \begin{cases} C_2, & k = l,\ 1 \le k, l \le N-1 \\ \{1\}, & \text{otherwise.} \end{cases}$$

A complete set of primitive idempotents of $\mathbf{C}\,((C_N \times C_N) \leftthreetimes C_2)$ are

$$\frac{1}{N^2}\{\alpha_k\beta_k(1+t)/2,\ \alpha_k\beta_k(1-t)/2,\ \alpha_k\beta_l,\ 1 \le k,\ l \le N-1,\ k \ne l\}.$$

$\frac{1}{2N^2}\alpha_k\beta_k(1+t)$ and $\frac{1}{2N^2}\alpha_k\beta_k(1-t)$, $1 \le k \le N-1$ are of dimension 1, while $\frac{1}{N^2}\alpha_k\beta_l$, $1 \le k, l \le N-1$, $k \ne l$ are of dimension 2.

### 7.2.2 Basis of orthogonal idempotents

$$\frac{1}{N^2}\{ \quad \alpha_0\beta_0(1+t)/2,\ \alpha_1\beta_0,\ \ldots,\alpha_{N-1}\beta_0,$$
$$\alpha_0\beta_1,\ \alpha_1\beta_1(1+t)/2,\ \ldots,\alpha_{N-1}\beta_1,$$
$$\vdots$$
$$\alpha_0\beta_{N-1},\ \alpha_1\beta_{N-1}\ldots,\ \alpha_{N-1}\beta_{N-1}(1+t)/2,$$
$$\alpha_0\beta_0(1-t)/2,\ t\alpha_1\beta_0,\ \ldots,t\alpha_{N-1}\beta_0,$$
$$t\alpha_0\beta_1,\ \alpha_1\beta_1(1-t)/2,\ \ldots,t\alpha_{N-1}\beta_1,$$
$$\vdots$$
$$t\alpha_0\beta_{N-1},\ t\alpha_1\beta_{N-1}\ldots,\ \alpha_{N-1}\beta_{N-1}(1-t)/2\}.$$

The matrix $\Gamma = \Gamma((C_N \times C_N) \leftthreetimes C_2)$ of change of bases is unitary and has computational complexity of $4N^2 \log N$. $\Gamma$ block-diagonalizes the group convolution into blocks of sizes 1 or 2. The group convolution can be implemented by the following algorithm. For $f,\ g \in \mathbf{C}D_N$, let $h = fg$.

1. Compute $\hat{f} = \Gamma f$ and $\hat{g} = \Gamma g$.
2. Compute $\hat{h}$ by

$$\begin{aligned}
&\hat{h}(m,m,0) = \hat{f}(m,m,0)\hat{g}(m,m,0),\\
&\hat{h}(m,m,1) = \hat{f}(m,m,1)\hat{g}(m,m,1), \qquad 0 \le m \le N-1,\\
&\hat{h}(m,n,0) = \hat{f}(m,n,0)\hat{g}(m,n,0) + \hat{f}(m,n,1)\hat{g}(n,m,1),\\
&\hat{h}(m,n,1) = \hat{f}(m,n,0)\hat{g}(m,n,1) + \hat{f}(m,n,1)\hat{g}(n,m,0),\\
&\qquad\qquad 1 \le m,\ n \le N-1,\ m \ne n.
\end{aligned}$$

3. Compute $h = \Gamma^{-1}h$.

## 7.3 $(C_N \times C_N) \leftthreetimes C_3$

$$G = \langle a, b, t;\ a^N = b^N = t^3 = 1,$$
$$ab = ba, ta^m b^n t^2 = a^{-n}b^{n-m}\rangle.$$

$$(C_N \times C_N)^* = \{\alpha_k\beta_l : 0 \le k,\ l \le N-1\},$$

$$\alpha_k\beta_l = \sum_{m,\,n} exp(2\pi i\frac{mk+nl}{N})a^m b^n.$$

$$(C_3)^* = \{\tau_0,\, \tau_1,\, \tau_2\},$$

$$\begin{aligned}\tau_0 &= 1+t+t^2,\\ \tau_1 &= 1+wt+w^2t^2,\\ \tau_2 &= 1+w^2t+wt^2, \quad w = exp(2\pi i/3).\end{aligned}$$

## 7.4 $(C_N \leftthreetimes C_2) \times (C_N \leftthreetimes C_2)$

$$G = \langle a,b,s,t;\ a^N = b^N = s^2 = t^2,$$
$$ab = ba, at = ta, sb = bs, st = ts, sas = a^{-1}, tbt = b^{-1}\rangle.$$

Set

$$\sigma_0 = 1+s,\ \sigma_1 = 1-s \qquad \tau_0 = 1+t,\ \tau_1 = 1-t.$$

- $2 \not| N$

  1-dimensional idempotents :

  $$\{\alpha_0\beta_0\sigma_0\tau_0,\ \alpha_0\beta_0\sigma_0\tau_1,\ \alpha_0\beta_0\sigma_1\tau_0,\ \alpha_0\beta_0\sigma_1\tau_1\}$$

  2-dimensional idempotents :

  $$\{\alpha_m\beta_0\tau_0, \alpha_m\beta_0\tau_1, \alpha_0\beta_n\sigma_0, \alpha_0\beta_n\sigma_1, \quad 1 \le m,n \le N-1\}.$$

  4-dimensional idempotents :

  $$\{\alpha_m\beta_n : 1 \le m,\, n \le N-1\}.$$

- $N = 2M$

  1-dimensional idempotents:

  $$\{\alpha_0\beta_0\sigma_0\tau_0,\ \alpha_M\beta_0\sigma_0\tau_0,\ \alpha_0\beta_0\sigma_1\tau_0,\ \alpha_M\beta_0\sigma_1\tau_0,$$
  $$\alpha_0\beta_M\sigma_0\tau_0,\ \alpha_M\beta_M\sigma_0\tau_0,\ \alpha_0\beta_M\sigma_1\tau_0,\ \alpha_M\beta_M\sigma_1\tau_0,$$
  $$\alpha_0\beta_0\sigma_0\tau_1,\ \alpha_M\beta_0\sigma_0\tau_1,\ \alpha_0\beta_0\sigma_1\tau_1,\ \alpha_M\beta_0\sigma_1\tau_1,$$
  $$\alpha_0\beta_M\sigma_0\tau_1,\ \alpha_M\beta_M\sigma_0\tau_1,\ \alpha_0\beta_M\sigma_1\tau_1,\ \alpha_M\beta_M\sigma_1\tau_1\}.$$

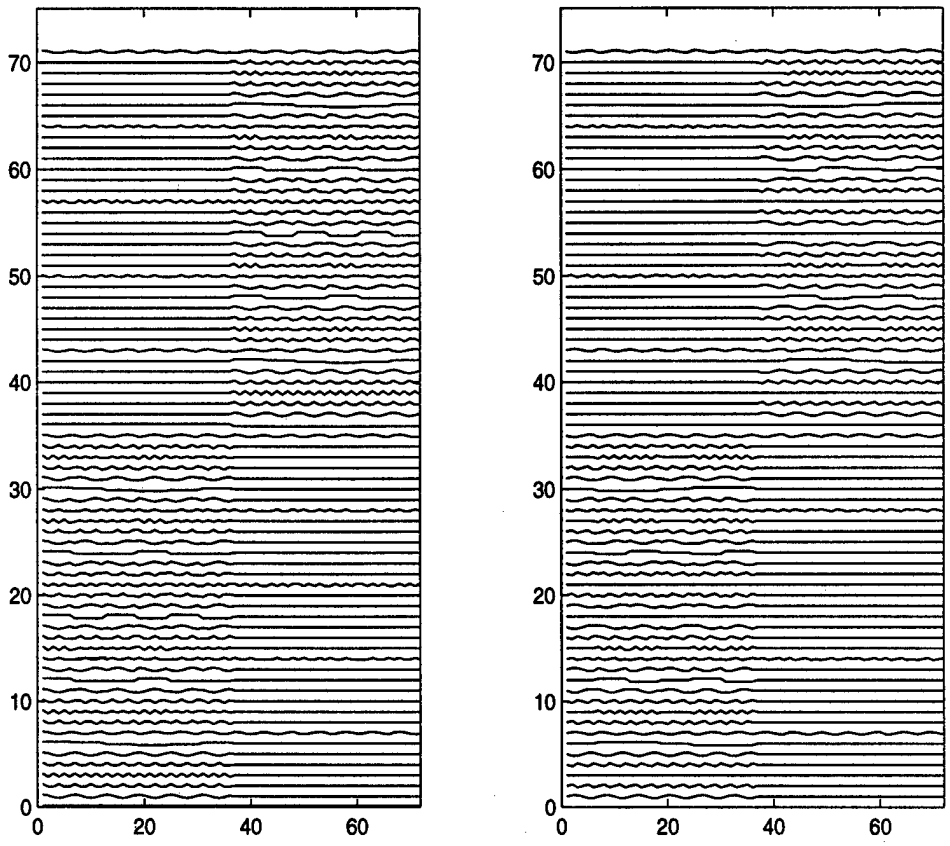
  2-dimensional idempotents:

  $$\{\alpha_m\beta_0\tau_0, \alpha_m\beta_M\tau_0, \alpha_m\beta_0\tau_1, \alpha_m\beta_M\tau_1, \alpha_0\beta_m\sigma_0, \alpha_M\beta_m\sigma_0, \alpha_0\beta_m\sigma_1, \alpha_M\beta_m\sigma_1 :$$
  $$1 \le m \le M-1,\ M+1 \le m,n \le N-1\}.$$

  4-dimensional idempotents:

  $$\{\alpha_m\beta_n : 1 \le m,\, n \le M-1,\ M+1 \le m,\, n \le N-1\}.$$

Figure 2: Profile of basis vectors for $\mathbf{C}\,(C_6 \times C_6) \leftthreetimes C_2)$




## 7.5 $(C_N \times C_N) \leftthreetimes (C_2 \times C_2)$

$$G = \langle a,\, b,\, s,\, t;\; a^N = b^N = s^2 = t^2,$$

$$ab = ba,\; st = ts,\; sa^m b^n s = a^n b^m,\; ta^m b^n t = a^{-m} b^{-n} \rangle.$$

$$(C_N \times C_N)^* = \{\alpha_k \beta_l : 0 \leq k, l \leq N-1\},$$

$$(C_2 \times C_2)^* = \{\sigma_0\tau_0,\, \sigma_1\tau_0,\, \sigma_0\tau_1,\, \sigma_1\tau_1\}.$$

- $2 \not| N$
- $N = 2M$.

  Centralizers:

$$C(\alpha_m\beta_n) = \begin{cases} (C_2 \times C_2)^*, & (m,n) = (0,0),\ (M,M), \\ \{1\,t\}, & (m,n) = (0,M),\ (M,0), \\ \{1,\ s\}, & (m,n) = (k,k), \\ \{1\}, & (m,n) = (k,l),\ (k,0),\ (0,k), \end{cases}$$

$$1 \le k, l \le M-1,\ M+1 \le k, l \le N-1.$$

1-dimensional idempotents:

$$\{\alpha_0\beta_0\sigma_0\tau_0,\ \alpha_M\beta_M\sigma_0\tau_0,\ \alpha_0\beta_0\sigma_1\tau_0,\ \alpha_M\beta_M\sigma_1\tau_0,$$

$$\alpha_0\beta_0\sigma_0\tau_1,\ \alpha_M\beta_M\sigma_0\tau_1,\ \alpha_0\beta_0\sigma_1\tau_1,\ \alpha_M\beta_M\sigma_1\tau_1\}.$$

2-dimensional idempotents:

$$\{\alpha_0\beta_M\sigma_0\tau_0,\ \alpha_M\beta_0\sigma_0\tau_0,\ \alpha_0\beta_M\sigma_0\tau_1,\ \alpha_M\beta_0\sigma_0\tau_1\},$$

$$\{\alpha_k\beta_k\sigma_0\tau_0, \alpha_k\beta_k\sigma_1\tau_0\},$$

$$\{\alpha_k\beta_{N-k}\sigma_0\tau_0,\ \alpha_k\beta_{N-k}\sigma_1\tau_1\},$$

$$1 \le k \le M-1,\ 1+M \le k \le N-1.$$

4-dimensional idempotents:

$$\{\alpha_k\beta_l,\ \alpha_k\beta_0, \alpha_0\beta_k; 1 \le k, l \le M-1,\ 1+M \le k, l \le N-1\}.$$

### 7.6 $(C_N \times C_N) \leftthreetimes C_4$

$$G = \langle a, b, t;\ a^N = b^N = t^4,$$

$$ab = ba, ta^m b^n t^3 = a^n b^{-m} \rangle.$$

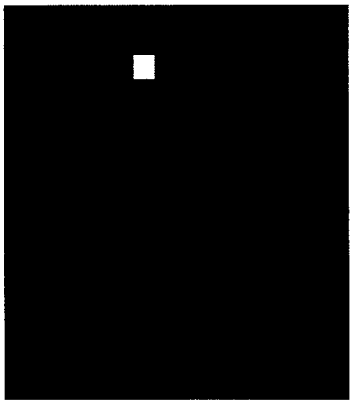
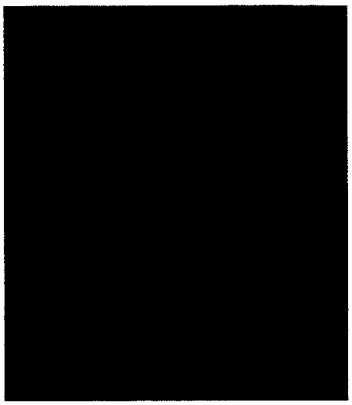
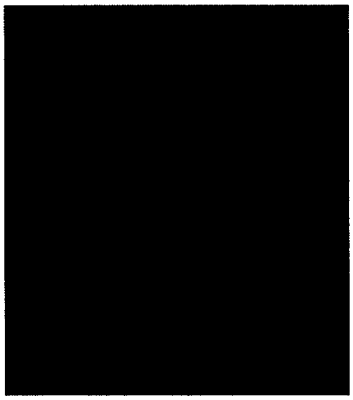
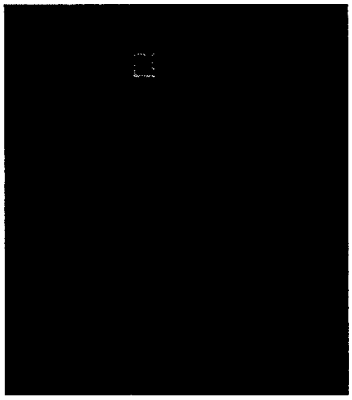
## 8 Results of numerical experiments

The following pictures illustrate the power of our methods to discriminate between object and noise in image data. Generally, we expect that image information will distribute over direct sum factors with noise more prominent in low dimensional factors and object more concentrated in high dimensional factors. In all but one of the illustrations the object can be recovered from the highest dimensional factor with significant noise reduction as measured by the signal to

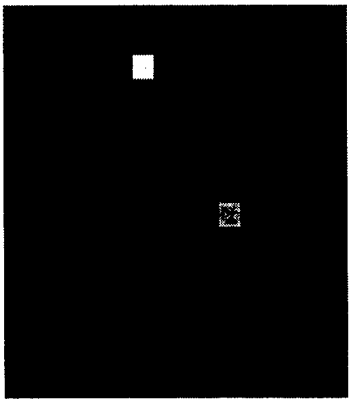
noise ratio (SNR). The one in which this is not the case, the second highest dimensional factor becomes most significant. The anomaly reflects the directional bias of the imaging model and emphasizes the importance of the imaging model as a tool for highlighting certain image characteristics.

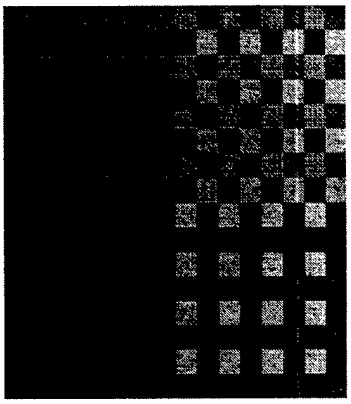
The two-dimensional images consists of delta functions, lines of delta functions and crossing lines of delta functions embedded in noise. Delta functions have pixel support and should be distinguished from regional boundaries. The noise is at 30% variance to the object. The imaging model indexes each coordinate direction by the dihedral group $C_8 \triangleleft C_2$ producing one, two and four-dimensional irreducible factors.

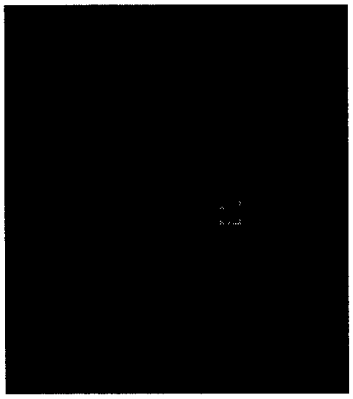
$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 2: Images in the following are 1) Single pixel of value 1, embedded in noise of values 0–0.25; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

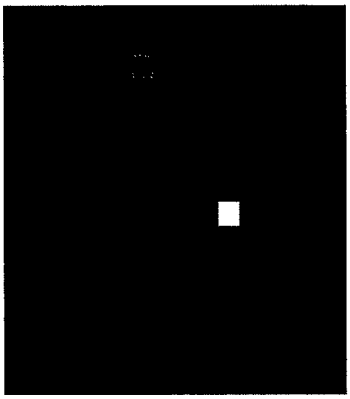





$G = (C_8 \triangleleft C_2) \times (C_8 \triangleleft C_2)$
Figure 3: Images in the following are 1) Two pixels of value 1 and 1.5, embedded in noise of values 0–0.5; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

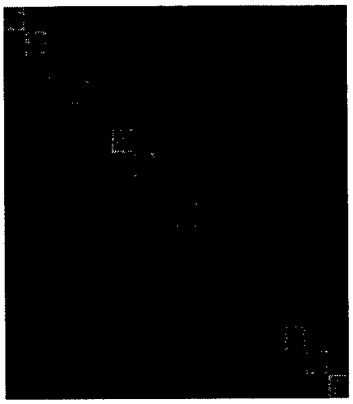


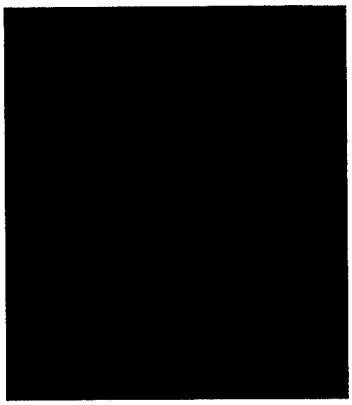


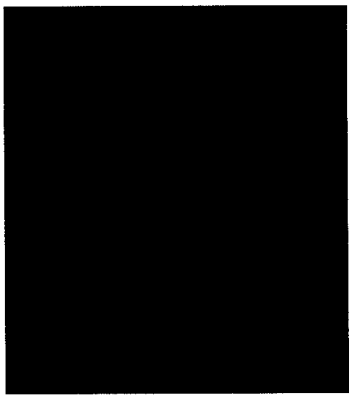


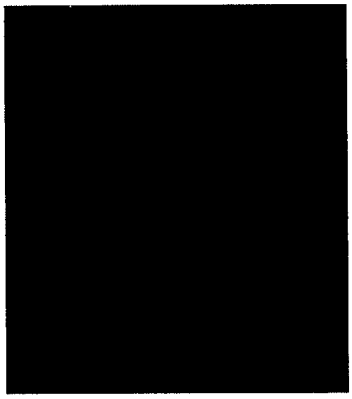


$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 4: Images in the following are 1) collection of pixels of value 1 embedded in noise of values 0–0.3; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

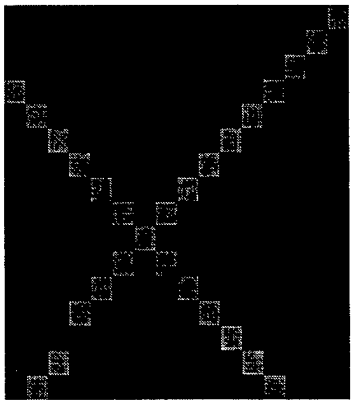
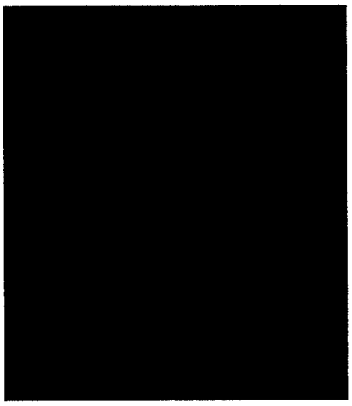
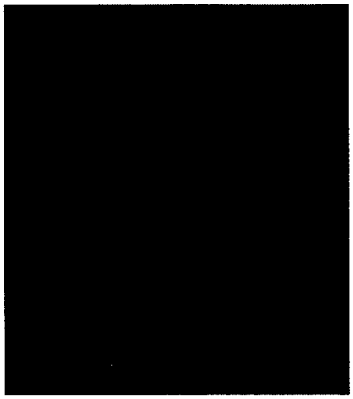
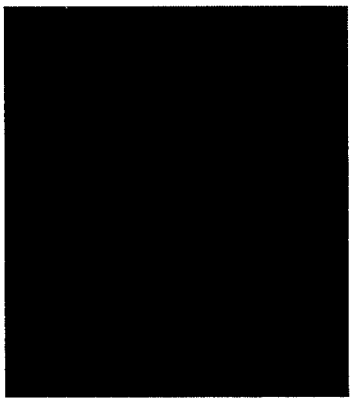




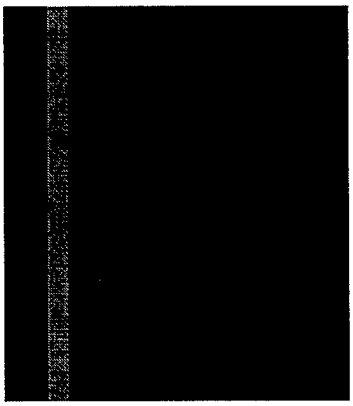


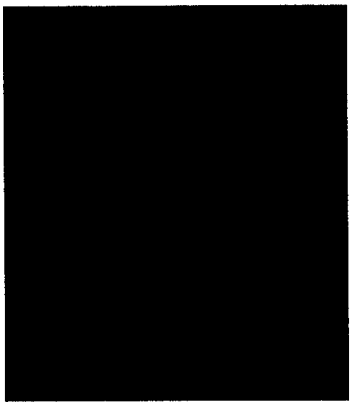


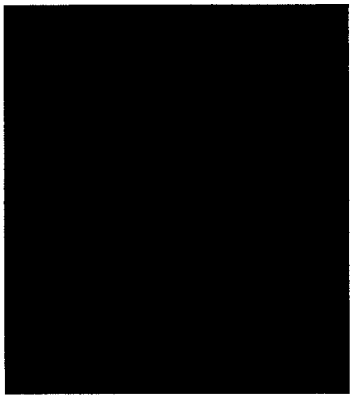
$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 5: Images in the following are 1) collection of pixels of value 1 embedded in noise of values 0–0.3; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

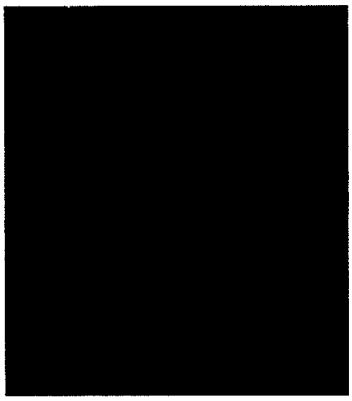





$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 6: Images in the following are 1) collection of pixels of value 1 embedded in noise of values 0–0.3; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.





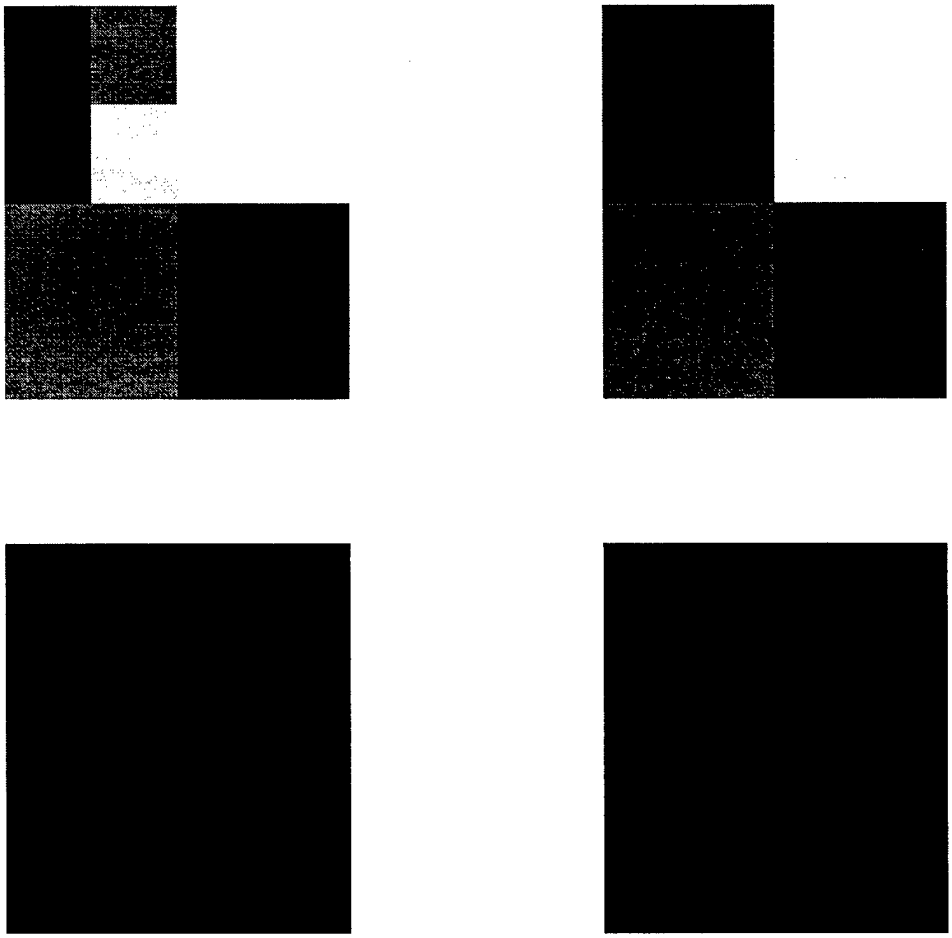




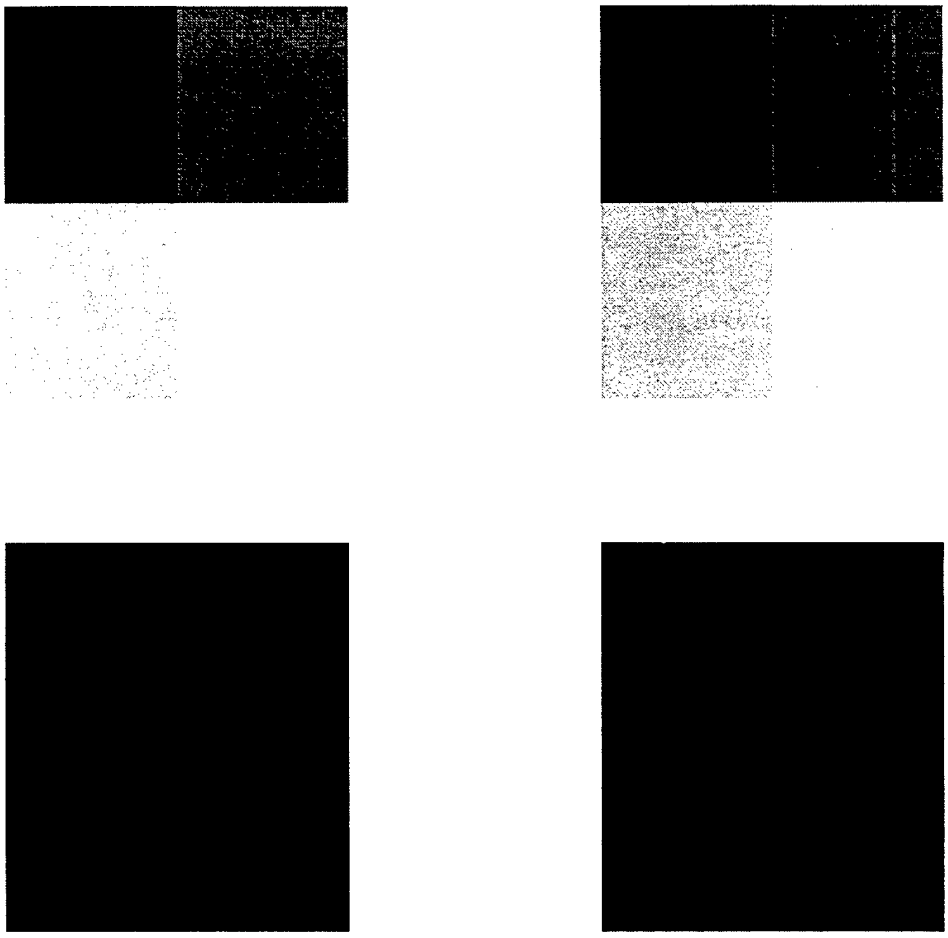
The following pictures illustrate the power of our methods as a data reduction tool for textures. Generally, textural information concentrates in low dimensional factors with higher dimensional factors representing textural changes. The bias of the imaging model affects which factors concentrate information but not the number of coefficients required to encode the information. Generally by slightly modifying the imaging model or by repositioning the texture, most information upto some resolution can be placed in the lowest dimensional factor. Since the number of coefficients required to encode this factor is a small fraction of the number of coefficients describing the texture, significant data reduction is possible. In Figure 12, we display the 16 coefficients required to describe a $32 \times 32$ coefficient texture.

$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$

Figure 7: Images in the quadrants are respectively 1) Simulated image of values 0, 1, 2 and 3; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

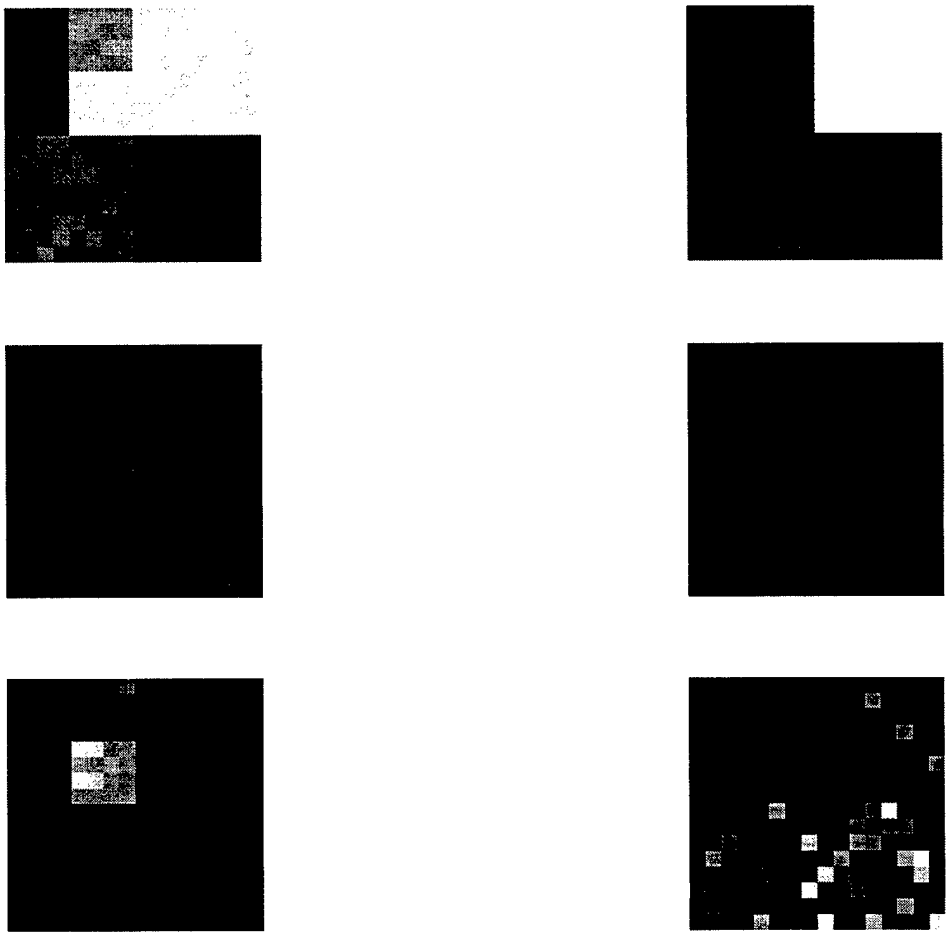


$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 8: Images in the quadrants are respectively 1) Simulated image of values 0–6; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.



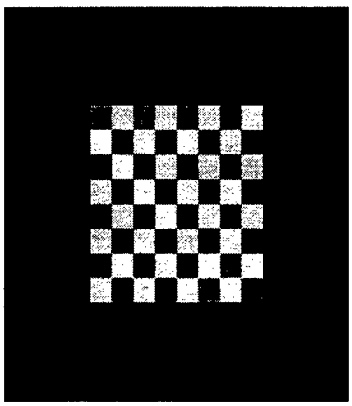
$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$

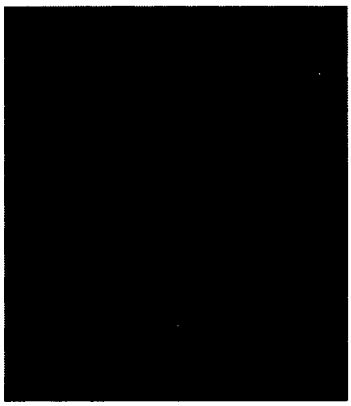
Figure 9: Images in the following are 1) Simulated image of values 0–6 describing texture with noise values of 0–.7 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors 4) 4-dimensional irreducible factors; 5) 2-dimensional irreducible factors uniformly multiplied by 3; 6) 4-dimensional irreducible factors multiplied uniformly multiplied by 10.

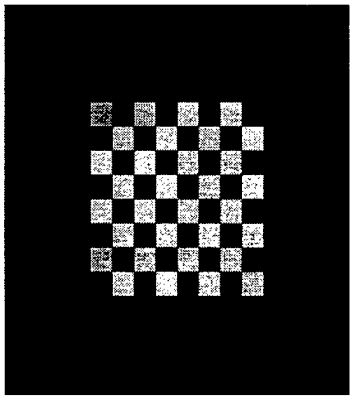


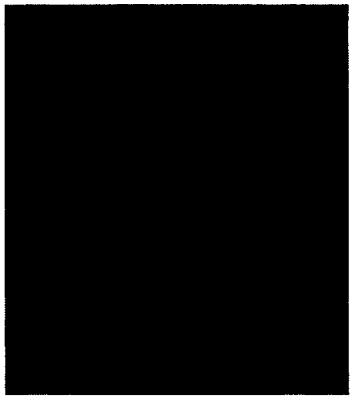
$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$

Figure 10: Images in the following are 1) Simulated image of values 0, 1, 2 describing texture with noise values of 0–0.25 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.



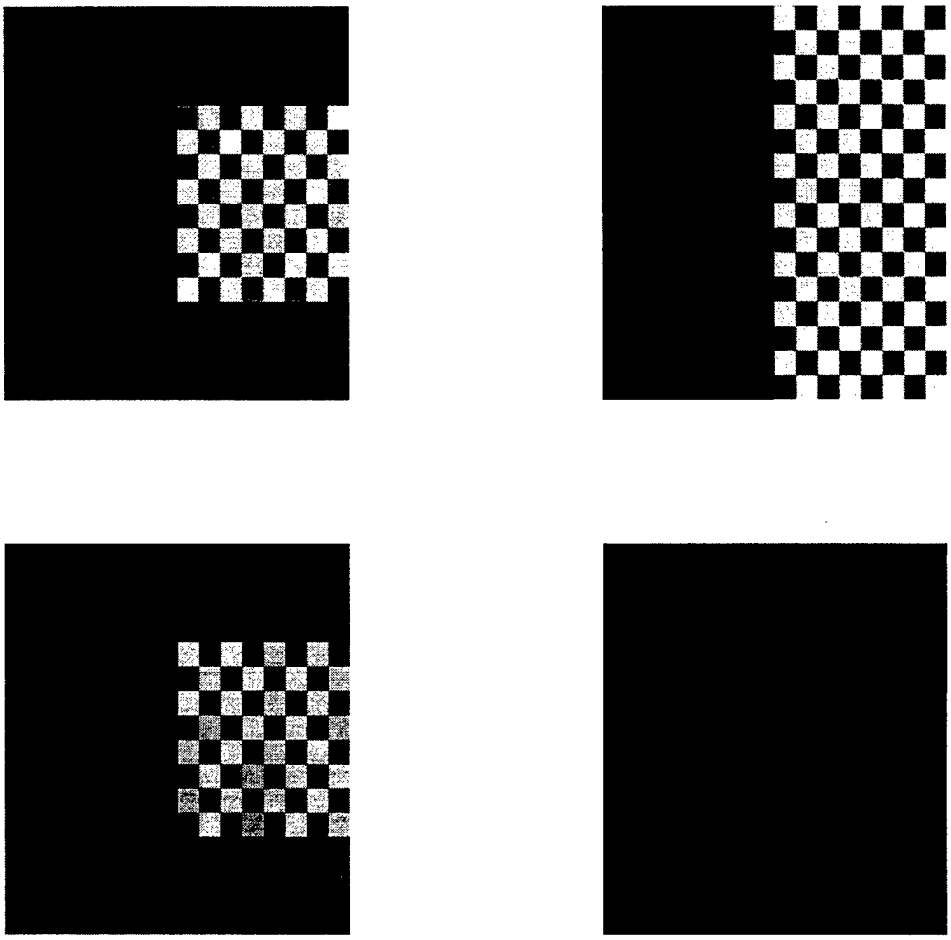




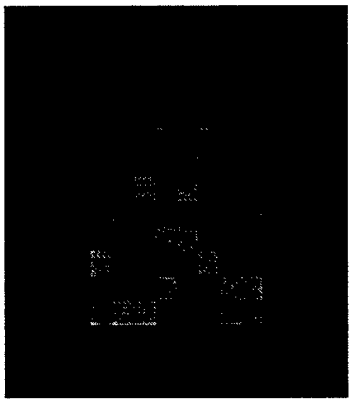


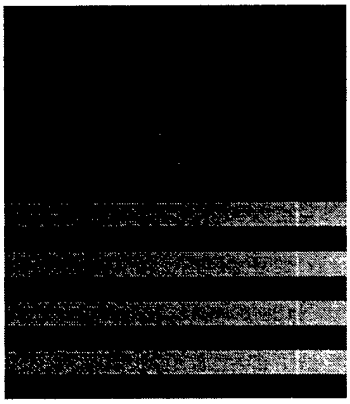
$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$

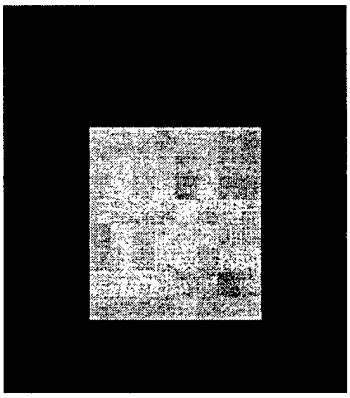
Figure 11: Images in the following are 1) Simulated image of values 0, 1, 2 describing texture with noise values of 0–0.25 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

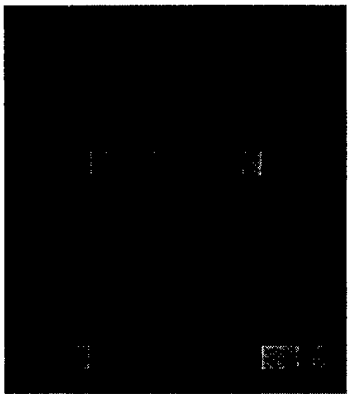


$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 12: Images in the following are 1) Simulated image of value 10 describing a square with noise values of 0–0.25 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

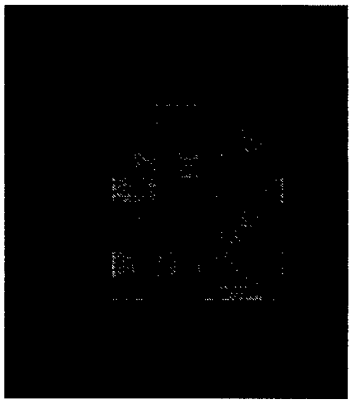


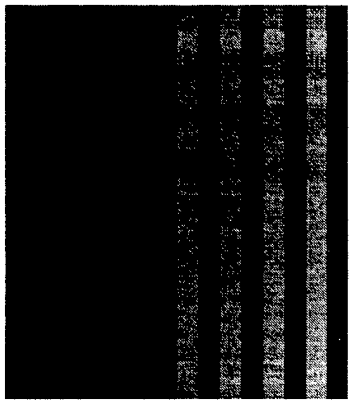


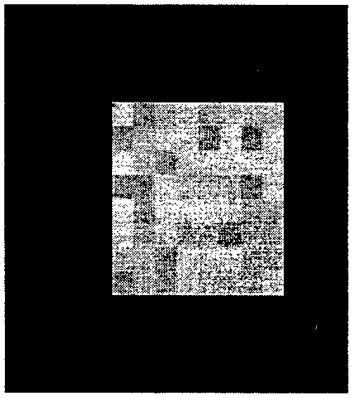


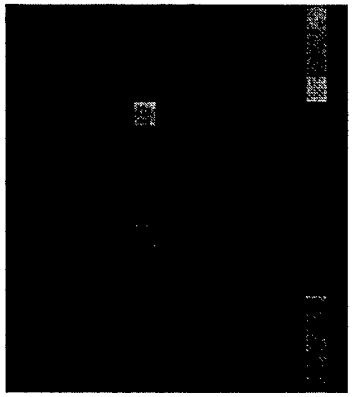


$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 13: Images in the following are 1) Simulated image of value 10 describing a square with noise values of 0–0.25 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

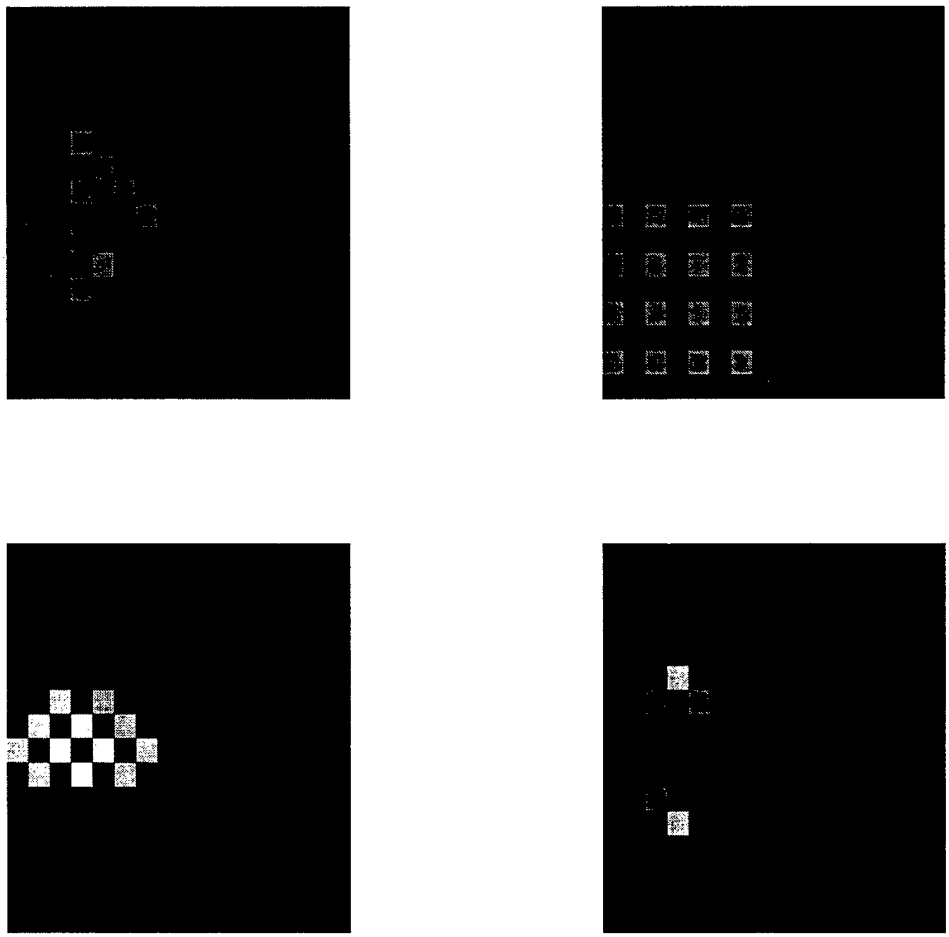




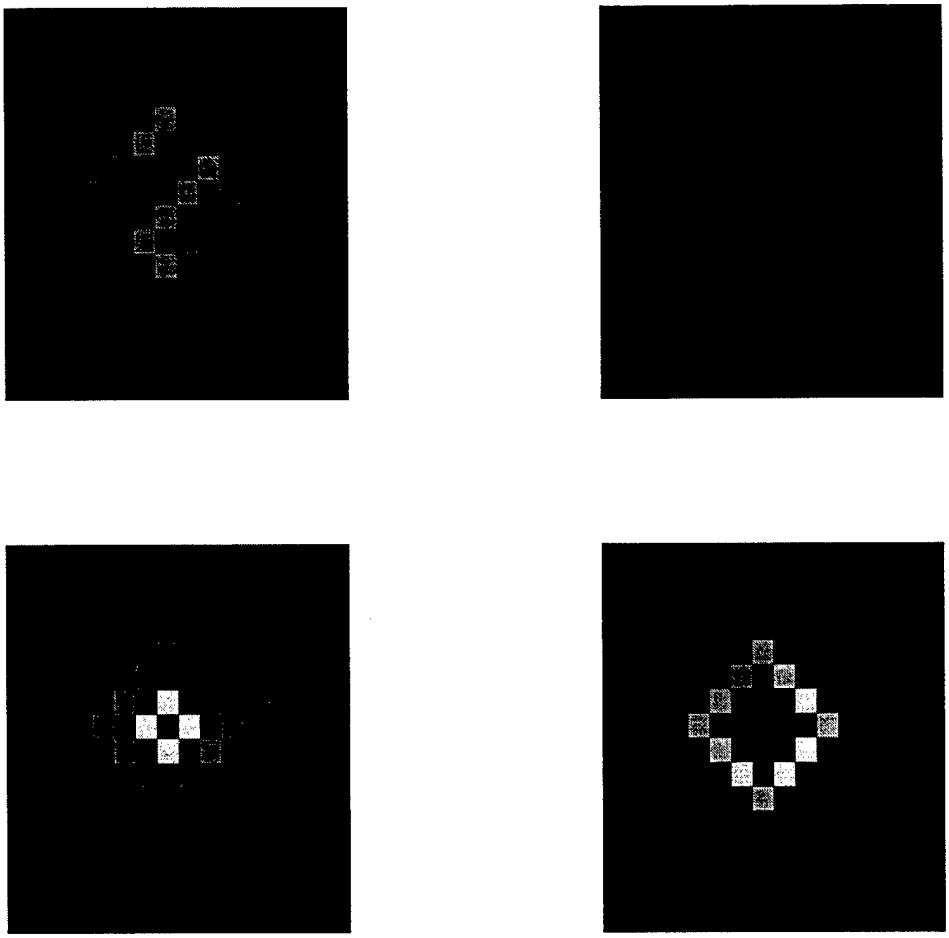




$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 14: Images in the following are 1) Simulated image of value 10 describing a square with noise values of 0–0.25 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.



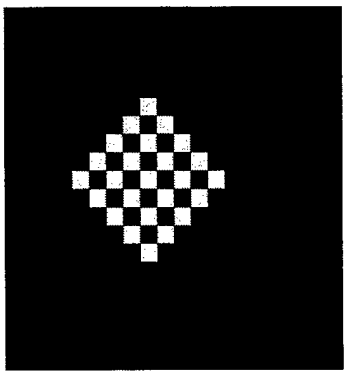
$G = (C_8 \leftthreetimes C_2) \times (C_8 \leftthreetimes C_2)$
Figure 15: Images in the following are 1) Simulated image of value 10 describing a square with noise values of 0–0.25 ; 2) 1-dimensional irreducible factors; 3) 2-dimensional irreducible factors and 4) 4-dimensional irreducible factors.

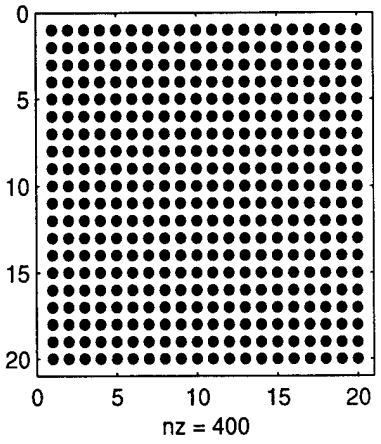


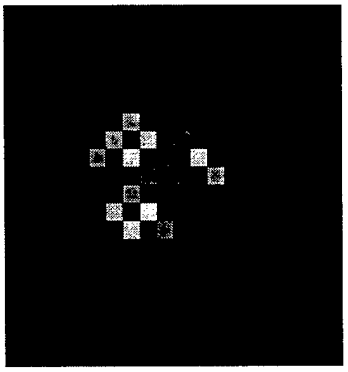
The following two figures illustrate the power of filtering in the coefficients of image expansions relative to the basis of translated idempotents to data compression and noise reduction.

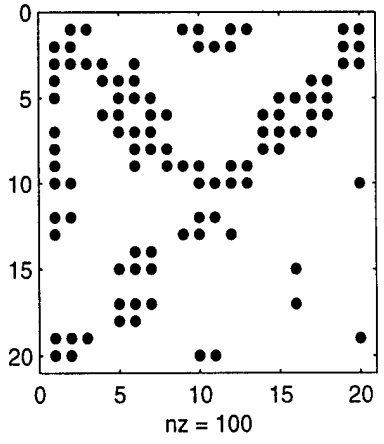
$G = (C_{10} \triangleleft C_2) \times (C_{10} \triangleleft C_2)$

Figure 16: Images in the following are 1) Simulated image of value 10 describing a square with noise values of 0–1 ; 2) Non-zeros coefficients describing the image; 3) Reconstruction using the 100 largest coefficients in the two larger dimensional irreducible factors; 4) Location of the non-zeros coefficients used in the reconstruction.







$G = (C_{10} \wr C_2) \times (C_{10} \wr C_2)$

Figure 17: Images in the following are 1) Simulated image of values of 5 and 10 describing a square with noise values of 0–1 ; 2) Non-zeros coefficients describing the image; 3) Reconstruction using the 8 largest coefficients in the one-dimensional irreducible factors; 4) Location of the non-zeros coefficients used in the reconstruction.